[JP,3073590,B]

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

---

(57) [Claim(s)]

[Claim 1] The electronic data protection system which protects the electronic data which are characterized by providing the following, and which were stored in the storage used with user side equipment based on the use consent from use consent person side equipment It is an electronic data decode key for said storage to store the medium specific number which specifies the storage concerned as a meaning in the enciphered encryption electronization data list, and for said use consent person side equipment decode the encryption electronization data stored in said storage. A consent information generation means to encipher said electronic data decode key based on the medium specific number stored in said storage, and to generate consent information The write-in means which writes the consent information generated by said consent information generation means in said storage A preparation and said user side equipment are a reading means read said consent information, encryption electronization data, and a medium specific number in said storage, a decode key generation means decode said consent information based on said medium specific number, and generate said electronic data decode key, and an electronic data decode means decode said encryption electronization data based on the electronic data decode key generated by said decode key generation means.

[Claim 2] Said consent information generation means and said decode key generation means It has a medium proper key generation means to generate a medium proper key based on the medium specific number stored in said storage, respectively. Said consent information generation means It has further a decode key encryption means to encipher said electronic data decode key based on the medium proper key generated by said medium proper key generation means. Said decode key generation means The electronic data protection system according to claim 1 characterized by having further a decode key decode means to decode said encryption electronization data based on the medium proper key generated by said medium proper key generation means.

[Claim 3] Said use consent person side equipment is equipped with a different electronic data decode key corresponding to two or more encryption electronization data stored in said storage, respectively. Said consent information generation means Only the electronic data decode key corresponding to the encryption electronization data to which use was permitted based on the medium specific number stored in said storage is enciphered, and consent information is generated. Said decode key generation means The electronic data protection system according to claim 1 or 2 characterized by generating the electronic data decode key corresponding to the encryption electronization data to which said consent information was decoded based on said medium specific number, and said use was permitted.

[Claim 4] Said storage is an electronic data protection system according to claim 1, 2, or 3 characterized by memorizing said medium specific number in the format in which rewriting by said user side equipment is impossible.

[Claim 5] Use consent person side equipment which performs use consent of the electronic data stored in the storage used with user side equipment characterized by providing the following The electronic data decode key for decoding the encryption electronization data stored in said storage A consent information generation means to encipher said electronic data decode key based on the medium specific number which specifies the storage concerned stored in said storage as a meaning, and to generate consent information, and the write-in means which writes the consent information generated by said consent information generation means in said storage

[Claim 6] Said consent information generation means is equipped the use consent person side according to claim 5 characterized by to have a medium proper key generation means generate a medium proper key based on the medium specific number stored in said storage, and a decode key encryption means encipher said electronic data decode key based on the medium proper key generated by said medium proper key generation means.

[Claim 7] It has a different electronic data decode key corresponding to two or more encryption electronization data stored in said storage, respectively, and equips the use consent person side according to claim 5 or 6 who does as the description that said consent information generation means enciphers only the electronic data decode key corresponding to the encryption electronization data to which use was permitted based on the medium specific number stored in said storage, and generates consent information.

[Claim 8] Said storage is equipped the use consent person side according to claim 5, 6, or 7 characterized by memorizing said medium specific number in the format in which rewriting by said user side equipment is impossible.

[Claim 9] User side equipment which uses the electronic data which are characterized by providing the following, and which were stored in the storage based on the use consent from use consent person side equipment A reading means to read

the medium specific number which specifies the storage concerned as a meaning, and the consent information enciphered by the enciphered encryption electronization data list in said storage A decode key generation means to decode said consent information based on said medium specific number, and to generate an electronic data decode key, and an electronic data decode means to decode said encryption electronization data based on the electronic data decode key generated by said decode key generation means

[Claim 10] Said decode key generation means is equipped the user side according to claim 9 characterized by having a medium proper key generation means to generate a medium proper key based on the medium specific number stored in said storage, and a decode key decode means to decode said encryption electronization data based on the medium proper key generated by said medium proper key generation means.

[Claim 11] Said decode key generation means decodes said consent information based on the medium specific number stored in said storage, and equips it the user side according to claim 9 or 10 characterized by generating the electronic data decode key corresponding to the encryption electronization data to which use of two or more encryption electronization data stored in the storage concerned was permitted.

[Claim 12] Said storage is equipped the user side according to claim 9, 10, or 11 characterized by memorizing said medium specific number in the format in which rewriting with the user side equipment concerned is impossible.

[Translation done.]

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Industrial Application] This invention relates to the electronic data protection system which prevents the unauthorized use of the computer software stored in the storage, an electronic publishing object, etc., use consent person side equipment, and user side equipment.

[0002] Generally software is easy to copy. Moreover, these illegal copy actions are performed frequently, and this obstructed the just profits of a software vendor, consequently the vicious circle that the price of software also must be set up more highly has arisen. Moreover, it is called for that it is published briskly, the problem of copyright becomes still more important, and an electronic publishing object in recent years prevents these programs and illegal copies of data.

[0003]

[Description of the Prior Art] Conventionally, as a protection method which protects a program, an electronic publishing object, especially software, as shown in drawing 14 , there is a method which generates the consent information 72 using the user specific number 91 of a user proper. The device number (device number of the proper given to the computer) is used for this conventional method as a user specific number 91. It enciphers and software is stored in the software storing medium 71. Moreover, as consent information 72, a user's proper key is generated from the user specific number 91, the software decode key 82 is enciphered with this proper key, the consent information 72 concerned is generated, and it stores in the software storing medium 71. By receiving sale of the encryption software 73 stored in the software storing medium 71, and the consent information 72, a user decodes the encryption software 73 for the software of a plaintext, and performs this. The conventional configuration and actuation of drawing 14 are explained briefly below.

[0004] Drawing 14 shows the explanatory view of the conventional technique. In drawing 14 , the software storing medium 71 is the medium which stores the consent information 72 which enciphered the encryption software 73 and the software decode key 82 which were enciphered, for example, a magneto-optic disk, and is a medium of the object which a user purchases from a sale side.

[0005] The consent information 72 is information which decodes the encryption software 73 and is made into the software of a plaintext, and enciphers the software decode key 82. The encryption software 73 enciphers software. There are the individual key generation 81, the software decode key 82, an encryption circuit 83, etc. in the sale side of consent information. The individual key generation 81 generates the individual key of a user proper based on the user specific number (for example, device number) 91 of a user computer. The software decode key 82 is a key for decoding the encryption software 73 for the software of the original plaintext. The encryption circuit 83 is a circuit which generates the consent

information 72 which enciphered the software decode key 82 with the individual key of the user proper generated by the individual key generation 81.

[0006] Moreover, there are the user specific number 91, the individual key generation 92, a decoder circuit 93, the software decode key 94, a decoder circuit 95, etc. in the user computer by the side of a user. The user specific number 91 is a number of a proper which a user computer has, for example, is the device number. The individual key generation 92 generates the individual key of a user proper based on the user specific number 91. A decoder circuit 93 decodes the consent information 72 read from the purchased software storing medium 71, and generates the software decode key 94.

[0007] The software decode key 94 is a key for decoding the encryption software 73 and decoding for the software of a plaintext. A decoder circuit 95 decodes the encryption software 73 read from the software storing medium 71 based on the software decode key 94, and makes it the software of the original plaintext. Loading of the software of this plaintext is carried out to the primary storage of a user calculating machine, and it is performed.

[0008] Below, actuation is explained.

(1) In the consent side of consent information, the individual key generation 81 generates the individual key of a user proper based on the user specific number 91 which a user computer has. Based on this generated individual key, it writes in the software storing medium 71 by which the encryption software 73 with which the encryption circuit 83 enciphered the software decode key 82, and enciphered software as consent information 72 was stored.

[0009] (2) A user purchases the software storing medium 71 by which the consent information 72 and the encryption software 73 were written in by (1), and equips a user computer with the software storing medium 71. Based on the user specific number (for example, device number) 91 of a proper which a user computer has, the individual key generation 92 generates the individual key of a user proper. Based on the individual key of this generated user proper, a decoder circuit 93 decodes the consent information 72 read from the purchased software storing medium 71, and generates the software decode key 94. Next, a decoder circuit 95 decodes the encryption software 73 read from the software storing medium 71 based on this generated software decode key 94, and generates the software of a plaintext. Loading of the software of this generated plaintext is carried out to a primary storage, and it is performed.

[0010]

[Problem(s) to be Solved by the Invention] The user specific number 91 is used for the conventional protection method of the configuration of drawing 14 mentioned above, and the specific number of a computer or the specific number of portable hardware is usually used for it. Since the consent information 72 will have given consent of activation to the computer and it becomes impossible to perform it only by this computer, when the specific number of a computer is used, even if it is a valid user, the problem that activation becomes impossible has arisen on a different computer. Moreover, transfer of software cannot be performed, either.

[0011] Moreover, when the specific number of portable hardware is used, the interface with the hardware itself and a computer needed to be established, and since the cost accompanying operation increases, the problem that operation becomes difficult has arisen.

[0012] This invention aims at carrying out to the ability only of the electronic data which the medium specific number was given to the medium of electronic data, the consent used to this medium specific number was given, and it was stored in the medium of normal, and consent gave being performed since these problems are solved.

[0013]

[Means for Solving the Problem] In order to attain the above-mentioned purpose, the electronic data protection system concerning invention of claim 1 In the electronic data protection system which protects the electronic data stored in the storage used with user side equipment based on the use consent from use consent person side equipment said storage The medium specific number which specifies the storage concerned as a meaning is stored in the enciphered encryption electronization data list. Said use consent person side equipment The electronic data decode key for decoding the encryption electronization data stored in said storage, A consent information generation means to encipher said electronic data decode key based on the medium specific number stored in said storage, and to generate consent information, It has the write-in means which writes the consent information generated by said consent information generation means in said storage. Said user side equipment A reading means to read said consent information, encryption electronization data, and a medium specific number in said storage, A decode key generation means to decode said consent information based on said medium specific number, and to generate said electronic data decode key, It is

characterized by having an electronic data decode means to decode said encryption electronization data based on the electronic data decode key generated by said decode key generation means.

[0014] Moreover, the electronic data protection system concerning invention of claim 2 In invention of claim 1 said consent information generation means and said decode key generation means It has a medium proper key generation means to generate a medium proper key based on the medium specific number stored in said storage, respectively. Said consent information generation means It has further a decode key encryption means to encipher said electronic data decode key based on the medium proper key generated by said medium proper key generation means. Said decode key generation means It is characterized by having further a decode key decode means to decode said encryption electronization data based on the medium proper key generated by said medium proper key generation means.

[0015] Moreover, the electronic data protection system concerning invention of claim 3 In invention of claims 1 or 2 said use consent person side equipment It has a different electronic data decode key corresponding to two or more encryption electronization data stored in said storage, respectively. Said consent information generation means Only the electronic data decode key corresponding to the encryption electronization data to which use was permitted based on the medium specific number stored in said storage is enciphered, and consent information is generated. Said decode key generation means It is characterized by generating the electronic data decode key corresponding to the encryption electronization data to which said consent information was decoded based on said medium specific number, and said use was permitted.

[0016] Moreover, the electronic data protection system concerning invention of claim 4 is characterized by said storage memorizing said medium specific number in the format in which rewriting by said user side equipment is impossible in invention of claims 1, 2, or 3.

[0017] Moreover, the use consent person side equipment concerning invention of claim 5 In the use consent person side equipment which performs use consent of the electronic data stored in the storage used with user side equipment The electronic data decode key for decoding the encryption electronization data stored in said storage, A consent information generation means to encipher said electronic data decode key based on the medium specific number which specifies the storage concerned stored in said storage as a meaning, and to generate consent information, It is characterized by having the write-in means which writes the consent information generated by said consent information generation means in said storage.

[0018] Moreover, the use consent person side equipment concerning invention of claim 6 is characterized in invention of claim 5 by to be equipped said consent information generation means with a medium proper key generation means generate a medium proper key based on the medium specific number which stored in said storage, and a decode key encryption means encipher said electronic data decode key based on the medium proper key generated by said medium proper key generation means.

[0019] Moreover, it carries out the use consent person side equipment concerning invention of claim 7 being equipped with a different electronic data decode key corresponding to two or more encryption electronization data which store in said storage in invention of claims 5 or 6, respectively, and said consent information generation means enciphering only the electronic data decode key corresponding to the encryption electronization data to which use was permitted based on the medium specific number stored in said storage, and generating consent information as the description.

[0020] Moreover, the use consent person side equipment concerning invention of claim 8 is characterized by said storage memorizing said medium specific number in the format in which rewriting by said user side equipment is impossible in invention of claims 5, 6, or 7.

[0021] Moreover, the user side equipment concerning invention of claim 9 In the user side equipment which uses the electronic data stored in the storage based on the use consent from use consent person side equipment A reading means to read the medium specific number which specifies the storage concerned as a meaning, and the consent information enciphered by the enciphered encryption electronization data list in said storage, It is characterized by having a decode key generation means to decode said consent information based on said medium specific number, and to generate an electronic data decode key, and an electronic data decode means to decode said encryption electronization data based on the electronic data decode key generated by said decode key generation means.

[0022] Moreover, the user side equipment concerning invention of claim 10 is characterized by to be

equipped said decode key generation means with a medium proper key generation means generate a medium proper key based on the medium specific number stored in said storage, and a decode key decode means decode said encryption electronization data based on the medium proper key generated by said medium proper key generation means in invention of claim 9.

[0023] Moreover, the user side equipment concerning invention of claim 11 is characterized by for said decode key generation means to decode said consent information based on the medium specific number stored in said storage, and to generate the electronic data decode key corresponding to the encryption electronization data to which use of two or more encryption electronization data stored in the storage concerned was permitted in invention of claims 9 or 10.

[0024] Moreover, the user side equipment concerning invention of claim 12 is characterized by said storage memorizing said medium specific number in the format in which rewriting with the user side equipment concerned is impossible in invention of claims 9, 10, or 11.

[0025]

[Function] According to invention concerning this claim 1, the medium specific number which specifies the storage concerned as a meaning at the enciphered encryption electronization data list is stored in the storage. Use consent person side equipment An electronic data decode key is enciphered based on the medium specific number stored in the storage, and the consent information which generated and generated consent information is written in a storage. With user side equipment Consent information, encryption electronization data, and a medium specific number are read in a storage. Since it considered as things so that consent information might be decoded based on the read medium specific number and encryption electronization data might be decoded based on the electronic data decode key which generated and generated the electronic data decode key Only the encryption electronization data which were stored in the storage of normal and were able to give consent from use consent person side equipment can be used with user side equipment.

[0026] Moreover, while enciphering an electronic data decode key based on the medium proper key which generated and generated the medium proper key based on the medium specific number stored in the storage according to invention concerning claim 2 Since encryption electronization data are decoded based on the medium proper key which generated and generated the medium proper key based on the medium specific number stored in the storage, code reinforcement of an electronic data decode key can be made still higher.

[0027] Moreover, according to invention concerning claim 3, a different electronic data decode key corresponding to two or more encryption electronization data stored in a storage is formed in use consent person side equipment, respectively. While enciphering only the electronic data decode key corresponding to the encryption electronization data to which use was permitted based on the medium specific number stored in the storage and generating consent information Since the electronic data decode key corresponding to the encryption electronization data to which consent information was decoded based on the medium specific number, and use was permitted is generated, it can respond, also when it stores two or more electronic data in one storage.

[0028] Moreover, according to invention concerning claim 4, since [a storage] a medium specific number is memorized in the format in which rewriting by user side equipment is impossible, it can prevent the unauthorized use which copies the encryption electronization data memorized to the storage to other storages.

[0029] Moreover, the electronic data decode key for decoding the encryption electronization data stored in the storage according to invention concerning claim 5 is formed. Since an electronic data decode key is enciphered based on the medium specific number which specifies the storage concerned stored in the storage as a meaning and the consent information which generated and generated consent information is written in a storage Consent can be given only to the encryption electronization data stored in the storage of normal.

[0030] Moreover, since [according to invention concerning claim 6] an electronic data decode key is enciphered based on the medium proper key which generated and generated the medium proper key based on the medium specific number stored in the storage, code reinforcement of an electronic data decode key can be made still higher.

[0031] Moreover, since it carried out forming a different electronic data decode key corresponding to two or more encryption electronization data stored in a storage, respectively, enciphering only the electronic data decode key corresponding to the encryption electronization data to which use was permitted based on the medium specific number stored in the storage,

and generating consent information according to invention concerning claim 7, also when it stores two or more electronic data to one storage, it can respond.

[0032] Moreover, according to invention concerning claim 8, since [a storage] said medium specific number is memorized in the format in which rewriting by user side equipment is impossible, it can prevent the unauthorized use which copies the encryption electronization data memorized to the storage to other storages.

[0033] Moreover, the medium specific number which specifies the storage concerned as a meaning from a storage according to invention concerning claim 9, The consent information enciphered by the enciphered encryption electronization data list is read. Since consent information is decoded based on the read medium specific number and encryption electronization data are decoded based on the electronic data decode key which generated and generated the electronic data decode key Only the encryption electronization data which were stored in the storage of normal and were able to give consent from use consent person side equipment can be used.

[0034] Moreover, since [according to invention concerning claim 10] encryption electronization data are decoded based on the medium proper key which generated and generated the medium proper key based on the medium specific number stored in the storage, code reinforcement of an electronic data decode key can be made still higher.

[0035] Moreover, since [according to invention concerning claim 11] consent information is decoded based on the medium specific number stored in the storage and the electronic data decode key corresponding to the encryption electronization data to which use of two or more encryption electronization data stored in the storage concerned was permitted is generated, also when it stores two or more electronic data in one storage, it can respond.

[0036] Moreover, according to invention concerning claim 12, since [a storage] said medium specific number is memorized in the format in which rewriting with the user side equipment concerned is impossible, it can prevent the unauthorized use which copies the encryption electronization data memorized to the storage to other storages.

[0037] Drawing 1 is drawing showing the principle block diagram of this invention, and, specifically, a medium 1 stores the medium specific number 12 and the consent information 13 of a meaning on the enciphered encryption electronization data 14 and the medium proper concerned in drawing 1 .

[0038] The individual key generation 21 and 31 generates a medium individual key from the medium specific number 12. Encryption 23 enciphers the electronic data decode key 22 with a medium individual key. With a medium individual key, decode 32 decodes the consent information 13 and generates the electronic data decode key 33. With the electronic data decode key 33, decode 34 decodes the encryption electronization data 14, and generates the electronic data of a plaintext.

[0039] This invention writes the encryption electronization data 14 beforehand enciphered with the medium specific number 12 of a meaning in the medium 1, as shown in drawing 1 . Are a consent side and the individual key generation 21 generates a medium proper key based on the medium specific number 12 of the meaning of a medium. Encryption 23 enciphers the electronic data decode key 22 with this medium proper key. A medium proper key is generated on a basis. the medium specific number 12 into which it writes in a medium 1 as consent information 13, and is a use side, and the individual key generation 31 read this enciphered data from the medium 1 -- The consent information 13 which decode 32 read with this medium proper key is decoded, the original electronic data decode key 33 is generated, the encryption electronization data 14 which decode 34 read with this electronic data decode key 33 are decoded, and it is made to make it the electronic data of a plaintext.

[0040] Moreover, an electronic data decode key 22 different every encryption electronization data 14 stored in one medium 1 is matched. Only the electronic data decode key 22 of the encryption electronization data 14 which are a consent side and permit use is enciphered with a medium proper key, respectively. Only the encryption electronization data 14 corresponding to the consent information 13 which stored in the medium 1 as consent information 13, is a use side and was stored in this medium 1 are decoded, and it is made to make it the electronic data of a plaintext.

[0041] Moreover, he is a use side and is trying to write in the medium specific number 12 of the meaning of a medium proper with the gestalt which is not rewritable. Moreover, he is trying to encipher the sort wear or the various data (an alphabetic character, an image, voice data, etc.) which operate a calculating machine as encryption electronization data 14.

[0042] Therefore, by giving the medium 1 which stores the encryption electronization data 14 with the gestalt which cannot rewrite the medium specific

number 12 of a meaning, and giving the consent which uses electronic data to this medium specific number 12 While being able to enable use of only the encryption electronization data 14 which it was stored in the medium 1 of normal, and consent gave, transfer of the electronic data stored in the medium 1 is enabled, and it can be used, being able to load another computer with the medium 1 concerned.

[0043]

[Example] Below, drawing 13 is used from drawing 2 and the configuration and actuation of the example of this invention are explained to a detail. Here, the software used for a computer is explained to an example below as an example of the electronic data explained by drawing 1 .

[0044] Drawing 2 shows 1 example block diagram of this invention. In drawing 2 , the software storing medium 11 is a medium which stores the software which a consent side permits to a use side, for example, are media, such as a magneto-optic disk (disk with the capacity of hundreds of M bytes thru/or several G bytes). The medium specific number [not being rewritable] 12, the consent information 13 which gives consent of software to a use side, and the encryption software 15 which enciphered software are stored in this software storing medium 11 like illustration.

[0045] The medium specific number 12 is a number of a meaning medium proper [that it is not rewritable to the software storing medium 11]. This medium specific number 12 is written in the field which a user cannot rewrite, and it may be made for OS to manage it, and also although it is called OS, once it writes in beforehand in the form which is not rewritable or writes in, it may be uncorrectable.

[0046] A consent side is the information which gives consent of software to a use side, and the consent information 13 is code data which decode the encryption software 15 here (it explains in full detail using drawing 6 and drawing 7).

[0047] The encryption software 15 enciphers software (it explains in full detail using drawing 5 from drawing 3). The individual key generation 21, the software decode key 24, encryption 23, etc. are formed in the computer by the side of consent.

[0048] The individual key generation 21 generates a medium individual key based on the medium specific number 12 read from the software storing medium 11 (it explains in full detail using drawing 6). Encryption 23 enciphers the software decode key 24 with the medium individual key generated by the individual key generation 21. This enciphered code data is stored in the software storing medium 11 as consent information 13.

[0049] The individual key generation 31, decode 32, the software decode key 35, decode 34, etc. are formed in the computer by the side of use. The individual key generation 31 generates a medium individual key based on the medium specific number 12 read from the software storing medium 11 (it explains in full detail using drawing 6). this -- the individual key generation 21 by the side of consent -- the same -- a medium individual key is generated.

[0050] With the medium individual key generated by the individual key generation 31, decode 32 decodes the consent information 13 read from the software storing medium 11, and generates the software decode key 35 (it explains in full detail using drawing 8).

[0051] With the software decode key 35, decode 34 decodes the encryption software 15 read from the software storing medium 11, and generates the software of a plaintext (it explains in full detail using drawing 8). Software of this generated plaintext is performed.

[0052] Hereafter, the configuration and actuation of drawing 2 are explained to a detail one by one. Drawing 3 shows the flow chart at the time of software storing of this invention. This is a flow chart when storing in the software storing medium 11 the encryption software 15 and the enciphered consent information 13 which created software and was enciphered.

[0053] In drawing 3 , S1 creates software. This creates the software (various user programs) which a manufacturer stores in a software storing medium. S2 creates a software cryptographic key.

[0054] S3 is matched with software and stored in a cryptographic key managed table. This is matched with the software cryptographic key managed table 4 of drawing 5 like illustration, and the software name of the software created by S1 and the cryptographic key created by S2 are stored, and it generalizes and manages it.

[0055] S4 performs ejection of the software cryptographic key corresponding to the specified software. This takes out the software cryptographic key corresponding to the software name stored in a software storing medium from the software cryptographic key managed table 4 of drawing 5 .

[0056] S5 is the software cryptographic key taken out by S4, enciphers the software of a plaintext and generates encryption software. As shown in drawing 4 , this enciphers the part of the body of software with an encryption key among the created software name

and the body of software, and creates a software name and the body of encryption software like illustration. Using DES etc., substitution and bit transposition are repeated and the code at this time enciphers, as explained to the lower berth.

[0057] S6 stores encryption software in the storing medium by the side of a manufacturer. This saves the encryption software enciphered once, this saved encryption software is taken out after next time, and it omits encryption.

[0058] S7 reads encryption software and stores it in the software storing medium 11. S8 distinguishes whether the encryption software stored in the software storing medium 11 finished. In YES, it ends. In NO, S7 is repeated, it carries out and sequential storing of the encryption software of the directed software name is carried out at the software storing medium 11.

[0059] It is made the encryption software which created software and enciphered this by the above, and this is stored in the software storing medium 11. Drawing 4 shows the example of encryption of the software of this invention.

[0060] (a) of drawing 4 shows the situation of the code of software. Here, the software name which performs a role of an identifier is stored in a header. This header is not made into the object of encryption. It considers as the object of encryption, it enciphers with an encryption key, and the body of software creates the body of encryption software. The encryption at this time uses DES (Data Encryption Standerd) like illustration. This DES repeats substitution and bit transposition and performs a code.

[0061] (b) of drawing 4 shows the situation of encryption. According to DES, like illustration, encryption enciphers with an encryption key and generates the 64-bit same bit string about a 64-bit bit string. Decode is decoded to the 64-bit original bit string with a decode key.

[0062] Drawing 5 shows the example of storing of the encryption software of this invention. In drawing 5 , the software cryptographic key managed table 4 is a table which matches the created software name and the created cryptographic key, and carries out generalization management, as mentioned already by drawing 3 . A 64-bit cryptographic key is carried out to the software name which gave "ENC" showing software being enciphered at a pair, respectively, and it stores in this software cryptographic key managed table 4.

[0063] Hereafter, actuation is explained.

(1) Take out a software cryptographic key from the software cryptographic key managed table 4 about the plaintext software which it is going to store in a software storing medium.

[0064] (2) Encipher plaintext software by the software cryptographic key to which the encryption circuit 41 was passed. Encryption is enciphered using DES of drawing 4 .

[0065] (3) Store the enciphered encryption software in the software storing medium 11 as illustration encryption software 15. It carries out repeatedly until it ends about all the plaintext software that had this specified. Under the present circumstances, what is necessary is to take out this saved encryption software from next time or subsequent ones, and just to store in the software storing medium 11, once it saves the enciphered encryption software. Moreover, the medium specific number 12 is a meaning number peculiar to the software storing medium 11, as mentioned already, and it is written in in the form [not being rewritable]. Moreover, the cryptographic key of the concerned cryptographic key [a decode key and] stored in the software cryptographic key managed table 4 corresponds, when an object key number is used for the algorithm of encryption.

[0066] By the above, about plaintext software, the software cryptographic key which corresponds from the software cryptographic key managed table 4 is taken out, it enciphers using this, encryption software is created, and it stores in the software storing medium 11.

[0067] Drawing 6 shows the generation flow chart of the consent information on this invention. This is a flow chart which generates the consent information 13 which the software which it is going to permit enciphered, and is stored in the software storing medium 11.

[0068] In drawing 6 , S11 inputs the software name which it is going to permit. S12 picks out a software decode key from the decode key managed table 5. This picks out the decode key of the software name which is going to give consent from the software decode key managed table 5 of drawing 7 .

[0069] S13 performs ejection of a medium specific number. This reads the medium specific number of the software storing medium 11 which is going to write in consent information. S14 generates a medium individual key. As indicated on right-hand side, this generates the medium individual key enciphered with the private key about the medium specific number 12 of the plaintext read from the software storing medium 11, or generates the medium individual key enciphered with the secret algorithm

about the medium specific number 12 of a plaintext.

[0070] With a medium individual key, S15 enciphers a software decode key and generates consent information. About the software decode key of a plaintext, it enciphers with the medium individual key generated by S14, and this generates consent information, as indicated on right-hand side.

[0071] S16 stores the enciphered consent information which was generated by S15 in the software storing medium 11. By the above, the medium specific number 12 is read from the software storing medium 11 which stored the encryption software 15, a medium individual key is generated, the consent information 13 enciphered and enciphered with this medium individual key about the software decode key is generated, and it stores in the FUTOWEA storing medium 11. It means that this had stored the encryption software 15 and the enciphered consent information 13 in the software storing medium 11.

[0072] Drawing 7 shows the generation explanatory view of the consent information on this invention. In drawing 7 , in case the software decode key managed table 5 decodes the encryption software 15 and decodes it for the software of a plaintext, it matches a required software decode key with a software UEA name, and manages it. The same decode key as the software cryptographic key managed table 4 explained by drawing 5 is stored in this software decode key managed table 5. A 64-bit software decode key is stored in a pair corresponding to the software name which gave "ENC" showing being enciphered here, and each software. Actuation is explained.

[0073] (1) When selling consent information to a use side, read the medium specific number 12 from the software storing medium 11 first. This read medium specific number 12 is inputted into the individual key generation circuit 211, and a medium individual key is generated (S14 reference of drawing 6).

[0074] (2) The software decode key of software which it is going to sell to the next is picked out from the software decode key managed table 5, input into the encryption circuit 231, encipher with a medium individual key, and generate the illustration consent information 13. This consent information 13 makes a pair consent information enciphered as the software name which gave the identifier showing the enciphered purport of ENC, and stores it in the software storing medium 11 as consent information 13. Here, a software decode key and the algorithm (or private key) of the individual key generation circuit 211 protect with a safe means.

[0075] By the above, a consent side generates a medium individual key based on the medium specific number 12 read from the software storing medium 11, enciphers a software decode key based on this medium individual key, and stores it in the software storing medium 11 as consent information 13.

[0076] Drawing 8 shows the flow chart of software decode of this invention. This is a flow chart when equipping a calculating machine with the software storing medium 11 which the use side purchased, carrying out loading of the software to a primary storage, and performing it.

[0077] In drawing 8 , S21 receives the run command of software. S22 performs ejection of the medium specific number 12 from the software storing medium 11.

[0078] S23 generates a medium individual key. This generates the medium individual key enciphered with the private key about the medium specific number 12 taken out from the software storing medium 11 by S22, as indicated on right-hand side. Or a secret algorithm generates the medium individual key enciphered from the medium specific number 12.

[0079] S24 is the medium individual key generated by S23, decodes the consent information 13 read from the software storing medium 11, and generates a software decode key. As indicated on right-hand side, this is the medium individual key enciphered by S23, decrypts the consent information 13 which is a cipher, and generates the software decode key 35 of a plaintext.

[0080] S25 reads encryption software 15 from the software storing medium 11. S26 is a software decode key, decodes the encryption software 15 read by S25, and generates the software of a plaintext. As indicated on right-hand side, about the encryption software 15 of a cipher, this is decoded with the software decode key 35 generated by S24, and generates the software of a plaintext. S27 carries out software activation.

[0081] A medium individual key is generated from the medium specific number 12 taken out from the software storing medium 11 by the above corresponding to the software run command, the consent information 13 which picked out this medium individual key from the software storing medium 11 on the basis is restored, the software decode key 35 is generated, the encryption software 15 taken out from the software storing medium 11 with this software decode key 35 is decoded, and the software of a plaintext is generated. It becomes possible to carry out loading of the software of this plaintext to a primary storage, and to perform it.

[0082] Drawing 9 shows the explanatory view in the case of the program of this invention. This is an

explanatory view in the case of a program as electronic data. (a) of drawing 9 shows a whole block diagram.

[0083] In (a) of drawing 9 , a magneto-optic disk 6 is a medium which stores an encryption program etc., is equivalent to the software storing medium 11 of drawing 2 , and stores the medium specific number 12, the consent information 13, and the encryption program 16. This magneto-optic disk 6 is purchased from a consent side, and optical-magnetic disc equipment is equipped with it. Besides this magneto-optic disk 6, you may be storages, such as an optical disk, CD-ROM, FD and HD, a magnetic tape, and a cassette tape.

[0084] At the time of program instruction activation, a program loader 61 carries out loading of the decoded program which corresponds from a magneto-optic disk 6 to a primary storage 63, changes it into the condition which can be performed, and is the processing section equipped with the key generation (individual key generation 31) mentioned already, decode (decode 32 and 34), etc. here.

[0085] A primary storage 63 is RAM (memory which can be written) for developing the program of a plaintext which the program loader 61 took out from the magneto-optic disk 6, and decoded.

[0086] Below, according to the sequence shown in the flow chart of (b) of drawing 9 , actuation of the configuration of (a) of drawing 9 is explained. In (b) of drawing 9 , S31 receives program instruction activation.

[0087] A program loader 61 finds an executive program, takes out S32, and it decodes. S33 carries out memory expansion on a primary storage. This develops on a primary storage 63 and changes into the condition that it can operate the program of a plaintext decoded by S32.

[0088] Program execution of S34 is carried out. Pro URAMU of the plaintext developed on the primary storage 63 by S33 is performed. (c) of drawing 9 shows the activation explanatory view of the software (program) in a user computer.

[0089] (1) A user computer takes out the medium specific number 12 from the software storing medium 11, and generates the medium individual key inputted and enciphered in the individual key generation circuit 311 (S23 reference of drawing 8).

[0090] (2) About consent information 13 like the illustration taken out from the software storing medium 11, a decoder circuit 321 decodes with the medium individual key generated by (1), and generates a software decode key 351 (it corresponds to the software decode key 35) like illustration.

[0091] (3) About the encryption software 15 taken out from the software storing medium 11, a decoder circuit 341 decodes with the software decode key 351 generated by (2), and generates the software (program) of a plaintext. Software (program) of this plaintext is developed and performed to a primary storage 63.

[0092] Here, the encryption software 15 with which the consent information 13 is not stored cannot be decoded, and cannot be performed. Moreover, there is no medium specific number 12, or when the software storing medium 11 is copied to the injustice of other media, since it differs, the right software decode key 351 cannot be decoded from the consent information 13, and as a result, encryption software cannot be decoded for the software of a plaintext and cannot be performed. In addition, on a user computer, the algorithm of the individual key generation circuit 311 or a private key, the generated software decode key, and the decoded plaintext software protect with a safe means.

[0093] Drawing 10 shows the explanatory view in the case of the data of this invention. This is an explanatory view in the case of voice data etc. as electronic data at alphabetic data (text), such as data, for example, a publication etc., a notation, image data, and a pan.

[0094] (a) of drawing 10 shows a whole block diagram. In (a) of drawing 10 , a magneto-optic disk 6 is a medium which stores encryption data etc., is equivalent to the software storing medium 11 of drawing 2 , and stores the medium specific number 12, the consent information 13, and the encryption data 17. This magneto-optic disk 6 is purchased from a consent side, and optical-magnetic disc equipment is equipped with it. Besides this magneto-optic disk 6, you may be storages, such as an optical disk, CD-ROM, FD and HD, a magnetic tape, and a cassette tape.

[0095] The R/W module 64 is the processing section equipped with the key generation (individual key generation 31) which stores the decoded data which correspond from a magneto-optic disk 6 in a primary storage 63, and mentioned them already here at the time of a lead instruction execution, decode (decode 32 and 34), etc. A primary storage 63 is RAM (memory which can be written) for storing the data of a plaintext which the R/W module 64 picked out from the magneto-optic disk 6, and decoded.

[0096] Below, according to the sequence shown in the flow chart of (b) of drawing 10 , actuation of the

configuration of (a) of drawing 10 is explained.

[0097] In (b) of drawing 10 , S41 carries out application activation. S42 executes a data reading instruction. The R/W module 64 finds data, reads and decodes S43. S44 is stored on a primary storage. S45 performs display of data, and playback.

[0098] By the above, when there is a reading instruction of data by S42, the R/W module 64 takes out and decodes the encryption data 17 from a magneto-optic disk 6, the data of a plaintext are generated, and this is stored in a primary storage 63. And it takes out from a primary storage 63, and display as a character string of a publication on a display, an image is displayed, or it generates as voice. Below, actuation of the R/W module 64 is explained to a detail.

[0099] (c) of drawing 10 shows display/playback explanatory view of the data in a user calculating machine.

(1) A user calculating machine takes out the medium specific number 12 from the data storage medium 111, inputs and enciphers in the individual key generation circuit 311, and generates a medium individual key (S23 reference of drawing 8).

[0100] (2) About consent information 13 like the illustration taken out from the data storage medium 111, a decoder circuit 321 decodes with the medium individual key generated by (1), and generates a data decode key 352 (it corresponds to the software decode key 35) like illustration.

[0101] (3) About the encryption data 17 picked out from the data storage medium 111, a decoder circuit 341 decodes with the data decode key 352 generated by (2), and generates the data (alphabetic data, image data, voice data, etc.) of a plaintext. The data of this plaintext are stored in a primary storage 63, and it displays as the character string of a publication, an image, and a notation on a display, or generates as voice.

[0102] Drawing 11 shows the case where it applies to a ROM/RAM mixture mold magneto-optic disk. The magneto-optic disk of a ROM/RAM mixture mold has like illustration the field in which user rewriting is impossible, the field which can be written, and a read-only field / field only for R/W. Therefore, the medium specific number 12, the consent information 13, and the encryption software 15 are stored in these fields like illustration. Since this writes the medium specific number 12 in the field in which user rewriting is impossible, the peculiar medium specific number of the magneto-optic disk concerned can be given, and protection of this invention can be aimed at.

[0103] Drawing 12 shows the example in the case of storing the consent information on this invention in other storing media. In this case, only the medium specific number and encryption software of a meaning peculiar to a software storing medium are beforehand stored like illustration. And consent information is stored in another consent information storing medium. This is an example in the case of writing beforehand a medium specific number and encryption software (encryption data) in the medium without the field written [CD-ROM] in, and writing the consent information which gives consent of the CD-ROMs concerned etc. in the consent information storing media (for example, FLOPPY etc.) in which another writing is possible.

[0104] Drawing 13 shows the explanatory view in the case of storing two or more software of this invention in the medium of one sheet. This is an example in case two or more software (or data) is stored in the mass media (a magneto-optic disk, CD-ROM, etc.) of one sheet and carries out individual sale. In this case, software decode keys 1 and 2 ... Consent information 1 and 2 enciphered with the medium proper key about N, respectively ... N is generated and it stores in the software storing medium 11. And a user is the encryption software 1 and 2 stored in the software storing medium 11... If the software name of purchase hope is notified to a consent information sale side among N, it enciphers with the medium individual key which generated the software decode key corresponding to software from the medium specific number, and a consent information sale side is stored in the software storing medium 11 by making this into consent information. A user uses the encryption software which equipped with this software storing medium 11, and was purchased by making it the software of a plaintext, decoding. On the other hand, even if a user is going to use software without consent information, he cannot decode encryption software, and he cannot use it. Moreover, since the medium specific number of the software storing medium 11 cannot be copied even if it copies the consent information on other software storing media 11, right decode cannot be performed. This becomes possible to perform individual sale of software.

[0105]

[Effect of the Invention] As explained above, according to invention concerning claim 1, the medium specific number which specifies the storage concerned as the enciphered encryption electronization data list at a meaning is stored in the storage. Use consent person side equipment enciphers an electronic data decode

key based on the medium specific number stored in the storage, and generates consent information. The generated consent information is written in a storage. With user side equipment Consent information, encryption electronization data, and a medium specific number are read in a storage. Since it constituted so that consent information might be decoded based on the read medium specific number and encryption electronization data might be decoded based on the electronic data decode key which generated and generated the electronic data decode key The effectiveness that the electronic data protection system which can use only the encryption electronization data which were stored in the storage of normal and were able to give consent from use consent person side equipment with user side equipment is obtained is done so.

[0106] Moreover, while enciphering an electronic data decode key based on the medium proper key which generated and generated the medium proper key based on the medium specific number stored in the storage according to invention concerning claim 2 Since it constituted so that encryption electronization data might be decoded based on the medium proper key which generated and generated the medium proper key based on the medium specific number stored in the storage The effectiveness that the electronic data protection system which can make still higher code reinforcement of an electronic data decode key is obtained is done so.

[0107] Moreover, according to invention concerning claim 3, a different electronic data decode key corresponding to two or more encryption electronization data stored in a storage is formed in use consent person side equipment, respectively. While enciphering only the electronic data decode key corresponding to the encryption electronization data to which use was permitted based on the medium specific number stored in the storage and generating consent information Since it constituted so that the electronic data decode key corresponding to the encryption electronization data to which consent information was decoded based on the medium specific number, and use was permitted might be generated The effectiveness that the electronic data protection system which can be corresponded also when it stores two or more electronic data in one storage is obtained is done so.

[0108] Moreover, the effectiveness that the electronic data protection system which can prevent the unauthorized use by which the encryption electronization data memorized to the storage are copied to other storages since it constituted so that a medium specific number might be memorized in the format in which rewriting [according to invention concerning claim 4] according [a storage] to user side equipment is impossible is obtained is done so.

[0109] Moreover, the electronic data decode key for decoding the encryption electronization data stored in the storage according to invention concerning claim 5 is formed. Since it constituted so that an electronic data decode key might be enciphered based on the medium specific number which specifies the storage concerned stored in the storage as a meaning, consent information might be generated and the generated consent information might be written in a storage The effectiveness that the use consent person side equipment which can give consent only to the encryption electronization data stored in the storage of normal is obtained is done so.

[0110] Moreover, since according to invention concerning claim 6 it constituted so that an electronic data decode key might be enciphered based on the medium proper key which generated and generated the medium proper key based on the medium specific number stored in the storage, the effectiveness that the use consent person side equipment which can make still higher code reinforcement of an electronic data decode key is obtained is done so.

[0111] Moreover, according to invention concerning claim 7, a different electronic data decode key corresponding to two or more encryption electronization data stored in a storage is formed, respectively. Since it constituted so that only the electronic data decode key corresponding to the encryption electronization data to which use was permitted based on the medium specific number stored in the storage might be enciphered and consent information might be generated The effectiveness that the use consent person side equipment which can be corresponded also when it stores two or more electronic data in one storage is obtained is done so.

[0112] Moreover, the effectiveness that the use consent person side equipment which can prevent the unauthorized use by which the encryption electronization data memorized to the storage are copied to other storages since it constituted so that said medium specific number might be memorized in the format in which rewriting [according to invention concerning claim 8] according [a storage] to user side equipment is impossible is obtained is done so.

[0113] Moreover, the medium specific number which specifies the storage concerned as a meaning from a storage according to invention concerning claim 9, The

consent information enciphered by the enciphered encryption electronization data list is read. Since it constituted so that consent information might be decoded based on the read medium specific number and encryption electronization data might be decoded based on the electronic data decode key which generated and generated the electronic data decode key The effectiveness that the user side equipment which can use only the encryption electronization data which were stored in the storage of normal and were able to give consent from use consent person side equipment is obtained is done so.

[0114] Moreover, since according to invention concerning claim 10 it constituted so that encryption electronization data might be decoded based on the medium proper key which generated and generated the medium proper key based on the medium specific number stored in the storage, the effectiveness that the user side equipment which can make still higher code reinforcement of an electronic data decode key is obtained is done so.

[0115] Moreover, according to invention concerning claim 11, consent information is decoded based on the medium specific number stored in the storage. Since the electronic data decode key corresponding to the encryption electronization data to which use of two or more encryption electronization data stored in the storage concerned was permitted was generated and the method configuration of things was carried out The effectiveness that the user side equipment which can be corresponded also when it stores two or more electronic data in one storage is obtained is done so.

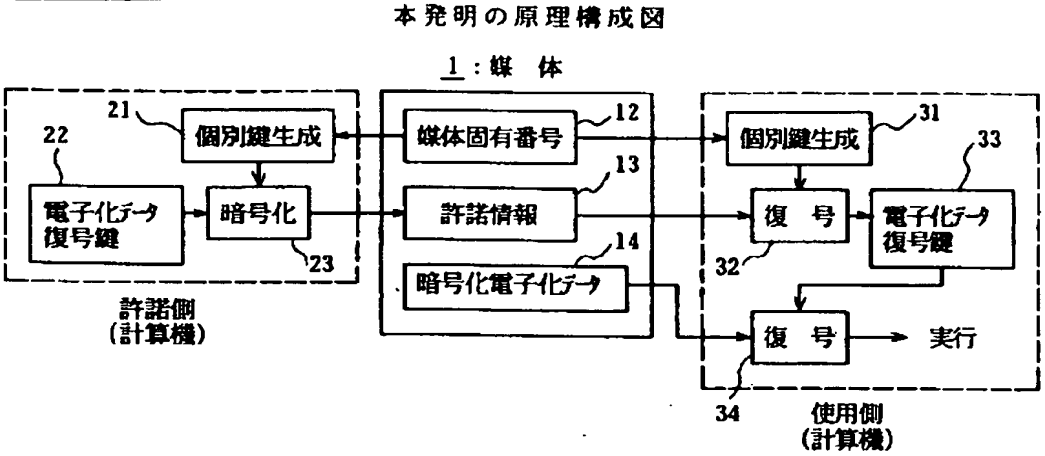
[0116] Moreover, according to invention concerning claim 12, since the storage was constituted so that said medium specific number might be memorized in the format in which rewriting with the user side equipment concerned is impossible, it does so the effectiveness that the user side equipment which can prevent the unauthorized use which copies the encryption electronization data memorized to the storage to other storages is obtained.

[Translation done.]

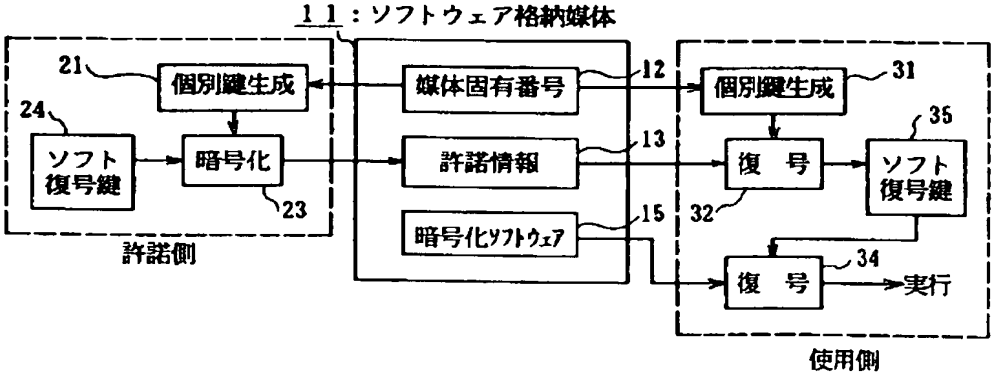
* NOTICES *

DRAWINGS

[Drawing 1]



[Drawing 2]

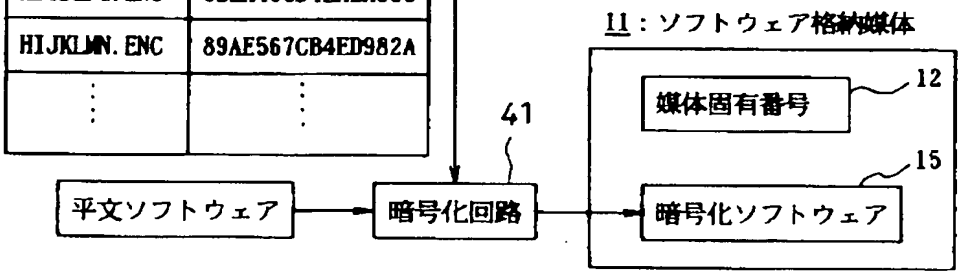


[Drawing 5]

本発明の暗号化ソフトウェアの格納例

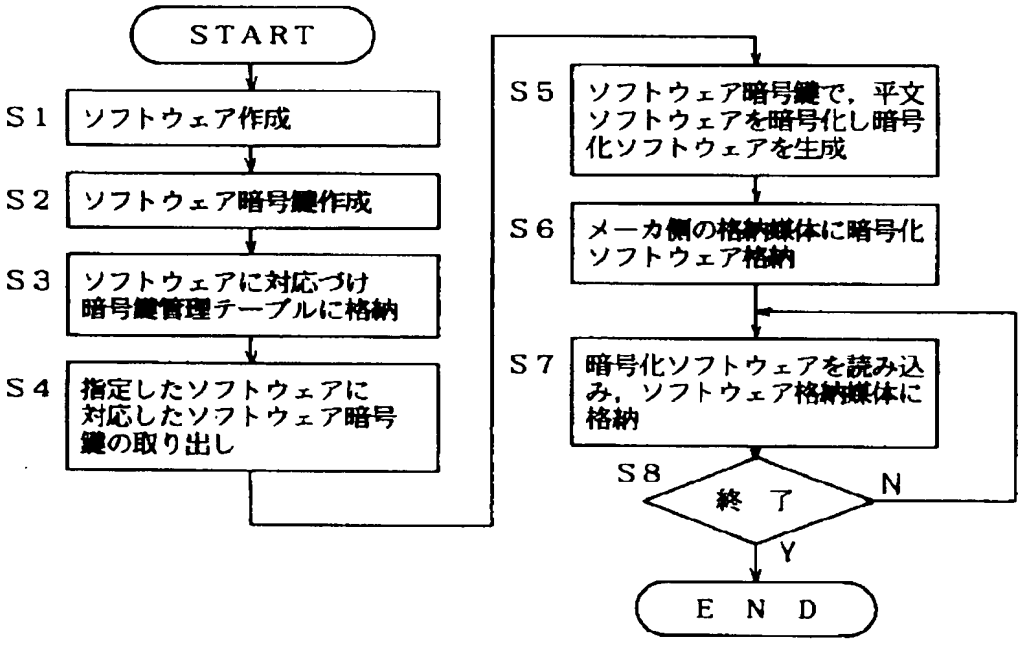
4：ソフトウェア暗号鍵管理テーブル

ソフトウェア名	暗号鍵
ABCDEFG.ENC	5BEA45CD4EA2A986
HIJKLMN.ENC	89AE567CB4ED982A
⋮	⋮



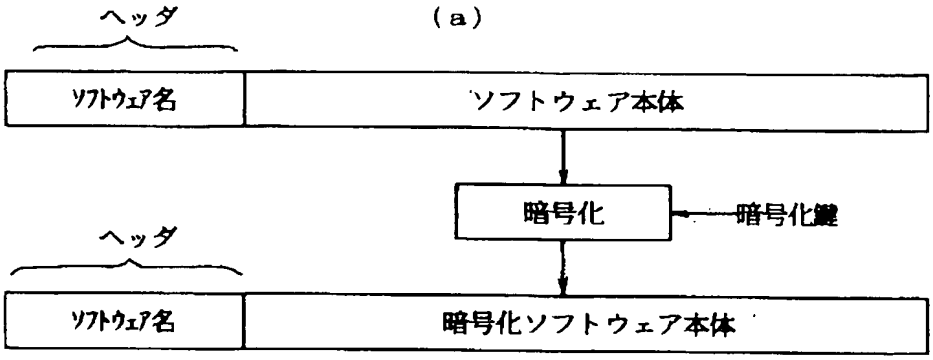
[Drawing 3]

本発明のソフトウェア格納時のフローチャート

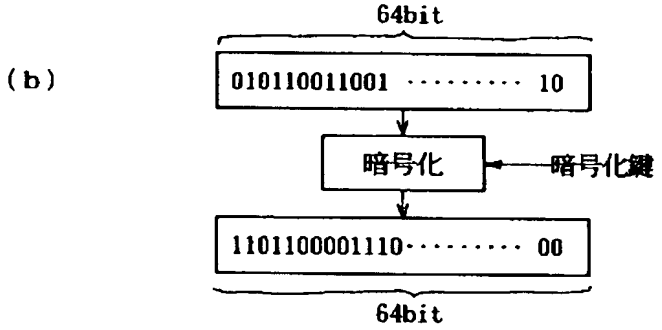


[Drawing 4]

本発明のソフトウェアの暗号化の例

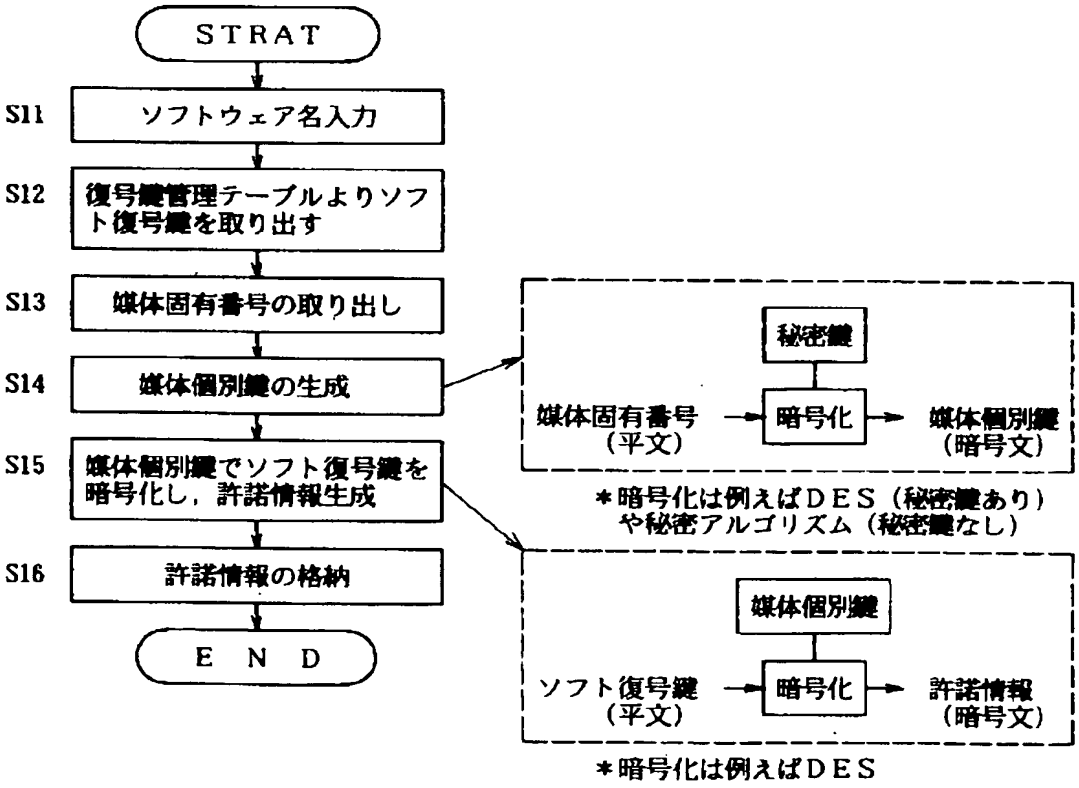


暗号化には，例えばＤＥＳ(Data Encryption Standerd)を用いる。
ＤＥＳは，換字とビット転置を繰り返し，暗号化を行う。



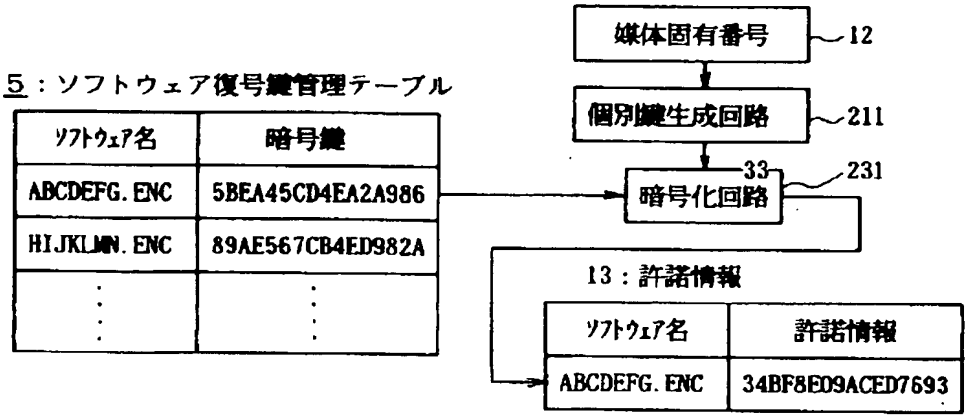
[Drawing 6]

本発明の許諾情報の生成フローチャート



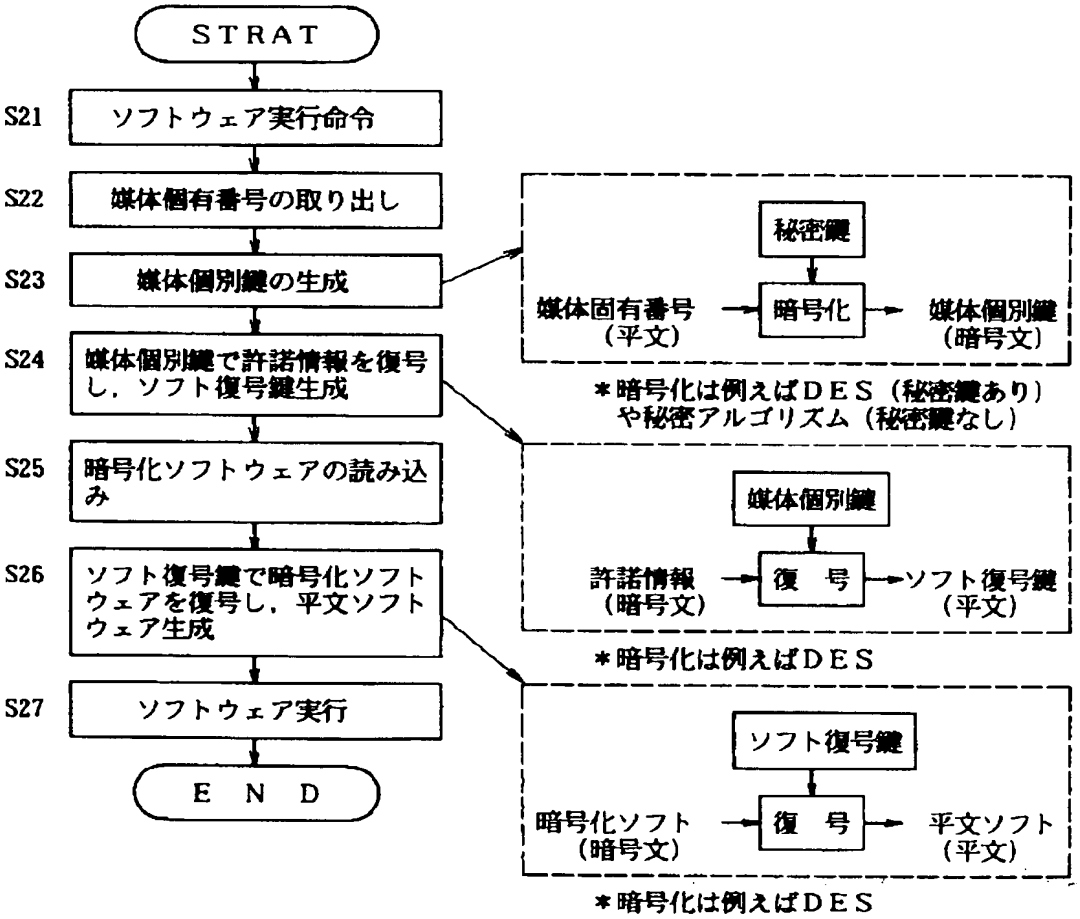
[Drawing 7]

本発明の許諾情報の生成説明図



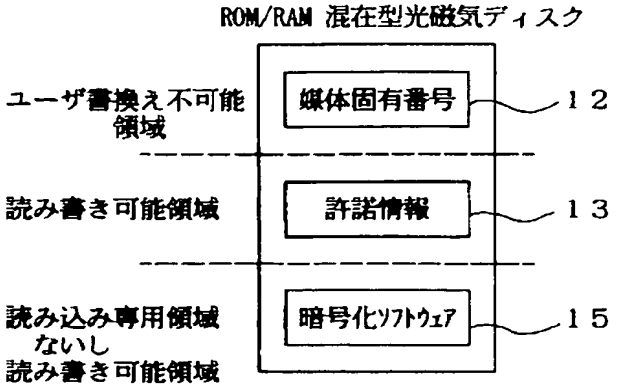
[Drawing 8]

本発明のソフトウェア復号のフローチャート



[Drawing 11]

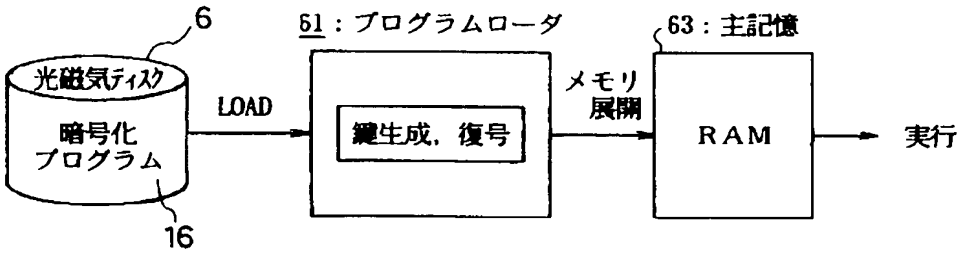
ROM/RAM 混在型光磁気ディスクに適用した場合



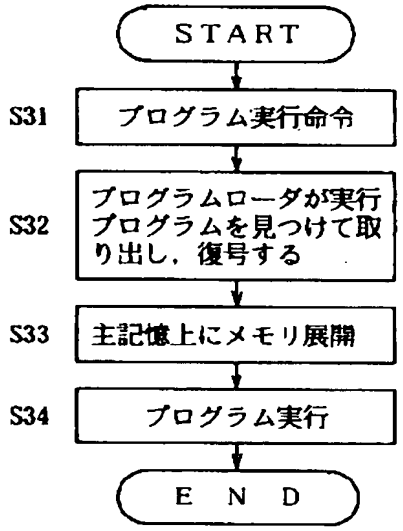
[Drawing 9]

本発明のプログラムの場合の説明図

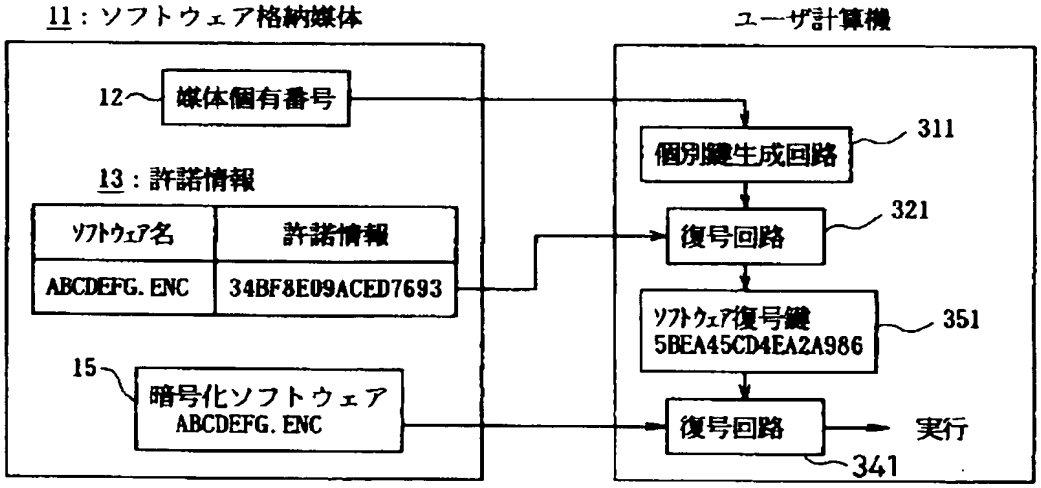
（ａ）全体構成図



（ｂ）動作フローチャート



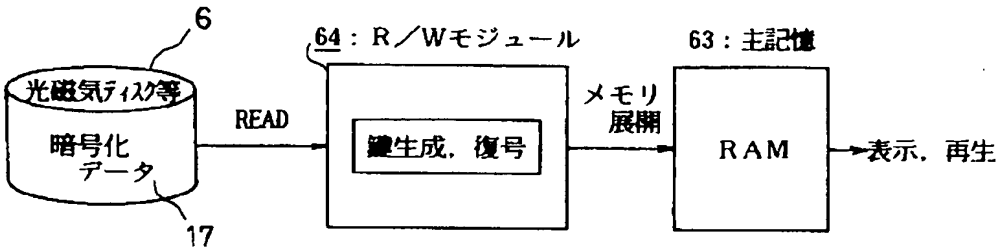
（ｃ）ユーザ計算機でのソフトウェアの実行説明図



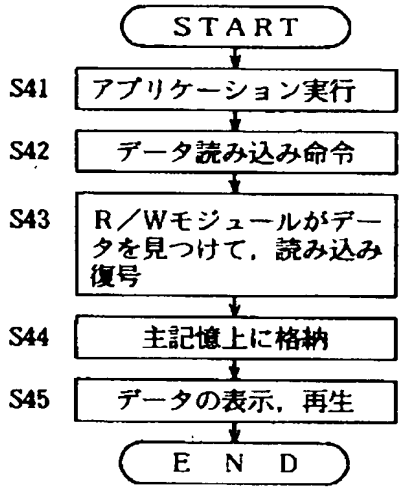
[Drawing 10]

本発明のデータの場合の説明図

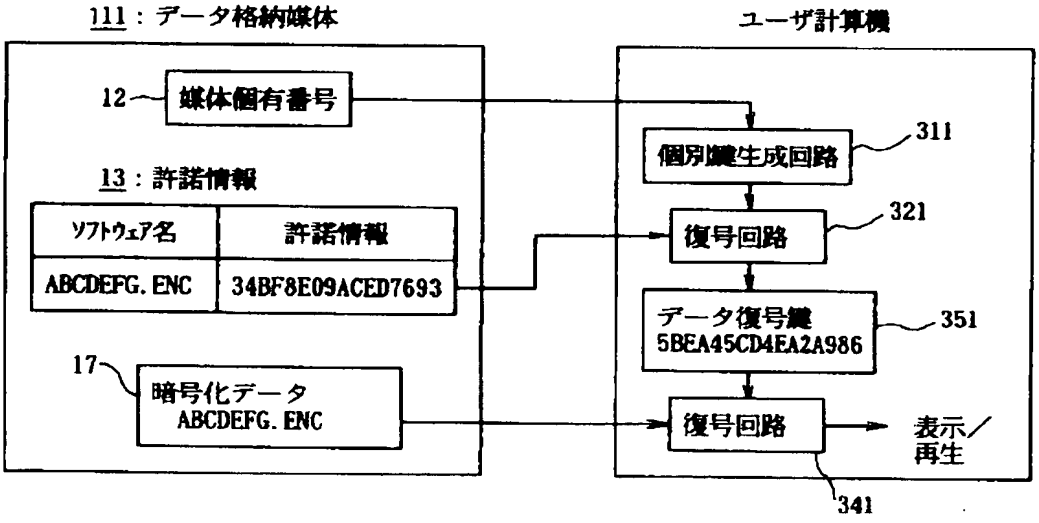
（a）全体構成図



（b）動作フローチャート

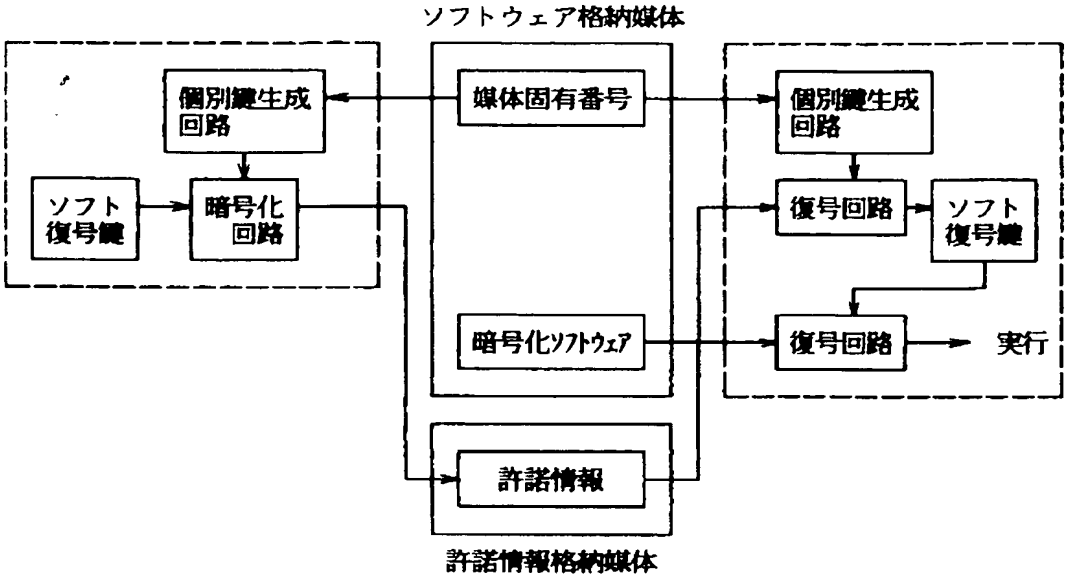


（c）ユーザ計算機でのデータの表示／再生説明図



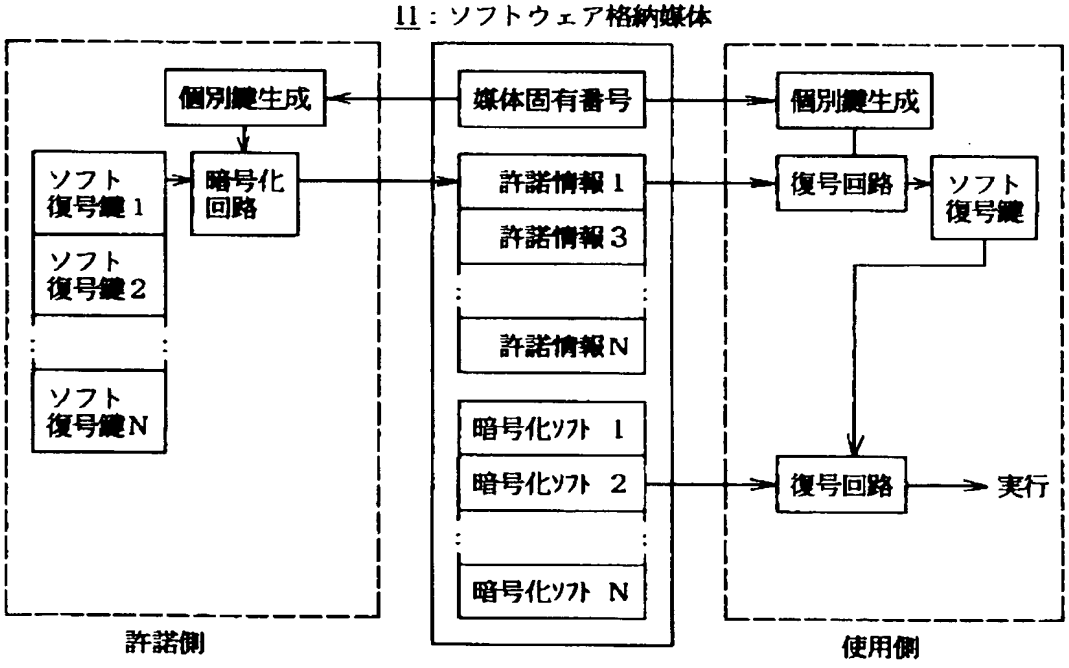
[Drawing 12]

本発明の許諾情報を他の格納媒体に格納する場合の例



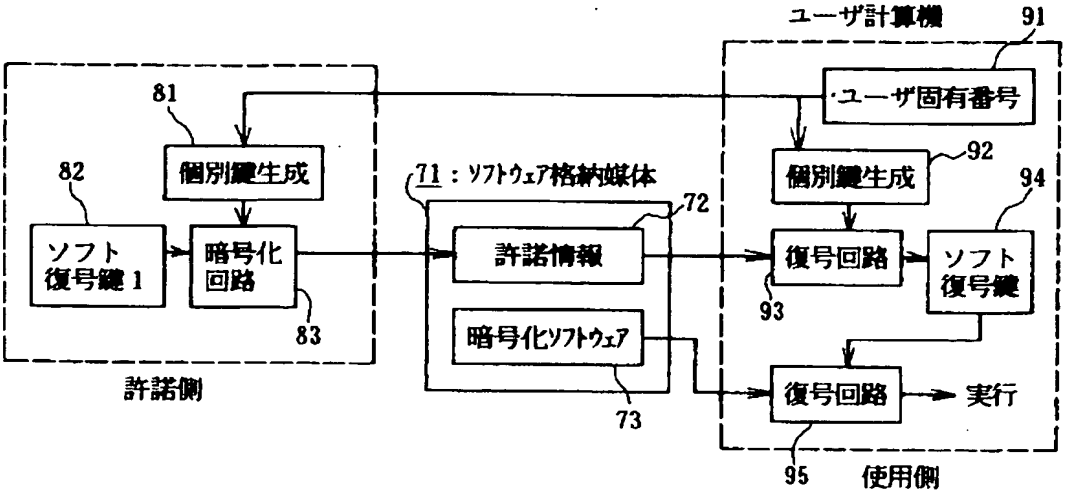
[Drawing 13]

本発明の複数のソフトを1枚の媒体に格納する場合の説明図



[Drawing 14]

従 来 技 術 の 説 明 図



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)特　許　公　報（Ｂ２）　(11)特許番号
特許第3073590号
(P3073590)

(45)発行日　平成12年８月７日(2000.8.7)　(24)登録日　平成12年６月２日(2000.6.2)

(51)Int.Cl.⁷	識別記号	FI	
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ
			３２０Ｅ
9/06	５５０	9/06	５５０Ｋ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ

請求項の数12(全 19 頁)

(21)出願番号　特願平4－58048

(22)出願日　平成４年３月16日(1992.3.16)

(65)公開番号　特開平5－257816

(43)公開日　平成５年10月８日(1993.10.8)

審査請求日　平成10年５月12日(1998.5.12)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　長谷部　高行
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　吉岡　誠
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(74)代理人　100089118
弁理士　酒井　宏明　(外１名)

審査官　梅村　勁樹

最終頁に続く

(54)【発明の名称】　電子化データ保護システム、使用許諾者側装置および使用者側装置

(57)【特許請求の範囲】

【請求項１】　使用者側装置で使用される記憶媒体に格納された電子化データを使用許諾者側装置からの使用許諾に基づいて保護する電子化データ保護システムにおいて、

前記記憶媒体は、暗号化した暗号化電子化データ並びに当該記憶媒体を一意に特定する媒体固有番号を格納し、

前記使用許諾者側装置は、前記記憶媒体に格納した暗号化電子化データを復号するための電子化データ復号鍵と、前記記憶媒体に格納した媒体固有番号に基づいて前記電子化データ復号鍵を暗号化して許諾情報を生成する許諾情報生成手段と、前記許諾情報生成手段により生成された許諾情報を前記記憶媒体に書き込む書込手段と、を備え、

前記使用者側装置は、前記記憶媒体から前記許諾情報、

暗号化電子化データおよび媒体固有番号を読み取る読取手段と、前記媒体固有番号に基づいて前記許諾情報を復号して前記電子化データ復号鍵を生成する復号鍵生成手段と、前記復号鍵生成手段により生成された電子化データ復号鍵に基づいて前記暗号化電子化データを復号する電子化データ復号手段と、

を備えたことを特徴とする電子化データ保護システム。

【請求項２】　前記許諾情報生成手段および前記復号鍵生成手段は、前記記憶媒体に格納した媒体固有番号に基づいて媒体固有鍵を生成する媒体固有鍵生成手段をそれぞれ備え、前記許諾情報生成手段は、前記媒体固有鍵生成手段により生成された媒体固有鍵に基づいて前記電子化データ復号鍵を暗号化する復号鍵暗号化手段をさらに備え、前記復号鍵生成手段は、前記媒体固有鍵生成手段により生成された媒体固有鍵に基づいて前記暗号化電子

化データを復号する復号鍵復号手段をさらに備えたことを特徴とする請求項１に記載の電子化データ保護システム。

【請求項３】　前記使用許諾者側装置は、前記記憶媒体に格納する複数の暗号化電子化データにそれぞれ対応する異なる電子化データ復号鍵を備え、前記許諾情報生成手段は、前記記憶媒体に格納した媒体固有番号に基づいて使用を許可された暗号化電子化データに対応する電子化データ復号鍵のみを暗号化して許諾情報を生成し、前記復号鍵生成手段は、前記媒体固有番号に基づいて前記許諾情報を復号して前記使用を許可された暗号化電子化データに対応する電子化データ復号鍵を生成することを特徴とする請求項１または２に記載の電子化データ保護システム。

【請求項４】　前記記憶媒体は、前記使用者側装置による書き替えが不可能な形式で前記媒体固有番号を記憶することを特徴とする請求項１、２または３に記載の電子化データ保護システム。

【請求項５】　使用者側装置で使用される記憶媒体に格納された電子化データの使用許諾をおこなう使用許諾者側装置において、

前記記憶媒体に格納した暗号化電子化データを復号するための電子化データ復号鍵と、

前記記憶媒体に格納した当該記憶媒体を一意に特定する媒体固有番号に基づいて前記電子化データ復号鍵を暗号化して許諾情報を生成する許諾情報生成手段と、

前記許諾情報生成手段により生成された許諾情報を前記記憶媒体に書き込む書込手段と、

を備えたことを特徴とする使用許諾者側装置。

【請求項６】　前記許諾情報生成手段は、前記記憶媒体に格納した媒体固有番号に基づいて媒体固有鍵を生成する媒体固有鍵生成手段と、前記媒体固有鍵生成手段により生成された媒体固有鍵に基づいて前記電子化データ復号鍵を暗号化する復号鍵暗号化手段と、を備えたことを特徴とする請求項５に記載の使用許諾者側装置。

【請求項７】　前記記憶媒体に格納する複数の暗号化電子化データにそれぞれ対応する異なる電子化データ復号鍵を備え、前記許諾情報生成手段は、前記記憶媒体に格納した媒体固有番号に基づいて使用を許可された暗号化電子化データに対応する電子化データ復号鍵のみを暗号化して許諾情報を生成することを特徴とする請求項５または６に記載の使用許諾者側装置。

【請求項８】　前記記憶媒体は、前記使用者側装置による書き替えが不可能な形式で前記媒体固有番号を記憶することを特徴とする請求項５、６または７に記載の使用許諾者側装置。

【請求項９】　記憶媒体に格納された電子化データを使用許諾者側装置からの使用許諾に基づいて使用する使用者側装置において、

前記記憶媒体から当該記憶媒体を一意に特定する媒体固有番号、暗号化された暗号化電子化データ並びに暗号化された許諾情報を読み取る読取手段と、

前記媒体固有番号に基づいて前記許諾情報を復号して電子化データ復号鍵を生成する復号鍵生成手段と、

前記復号鍵生成手段により生成された電子化データ復号鍵に基づいて前記暗号化電子化データを復号する電子化データ復号手段と、

を備えたことを特徴とする使用者側装置。

【請求項１０】　前記復号鍵生成手段は、前記記憶媒体に格納した媒体固有番号に基づいて媒体固有鍵を生成する媒体固有鍵生成手段と、前記媒体固有鍵生成手段により生成された媒体固有鍵に基づいて前記暗号化電子化データを復号する復号鍵復号手段と、を備えたことを特徴とする請求項９に記載の使用者側装置。

【請求項１１】　前記復号鍵生成手段は、前記記憶媒体に格納した媒体固有番号に基づいて前記許諾情報を復号して、当該記憶媒体に格納された複数の暗号化電子化データのうちの使用を許可された暗号化電子化データに対応する電子化データ復号鍵を生成することを特徴とする請求項９または１０に記載の使用者側装置。

【請求項１２】　前記記憶媒体は、当該使用者側装置での書き替えが不可能な形式で前記媒体固有番号を記憶することを特徴とする請求項９、１０または１１に記載の使用者側装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、記憶媒体に格納したコンピュータソフトウエアや電子出版物などの不正使用を防止する電子化データ保護システム、使用許諾者側装置および使用者側装置に関する。

【０００２】ソフトウェアは一般的にコピーが容易である。また、これらの不正コピー行為は、頻繁に行われており、これがソフトウェアベンダーの正当な利益を阻み、その結果、ソフトウェアの価格も高めに設定せざるを得ないといった悪循環が生じている。また、近年の電子出版物が盛んに出版されるようになってきており、著作権の問題はさらに重要となり、これらのプログラムやデータの不正コピーを防止することが求められている。

【０００３】

【従来の技術】従来、プログラムや電子出版物、特にソフトウェアを保護する保護方式として、図１４に示すように、ユーザ固有のユーザ固有番号９１を用いて許諾情報７２を生成する方式がある。この従来の方式は、ユーザ固有番号９１としてたとえば装置番号（計算機に付与された固有の装置番号）を用いる。ソフトウェアは、暗号化してソフトウェア格納媒体７１に格納する。また、許諾情報７２として、ユーザ固有番号９１からユーザの固有鍵を生成し、この固有鍵でソフト復号鍵８２を暗号化して当該許諾情報７２を生成し、ソフトウェア格納媒体７１に格納する。ユーザは、ソフトウェア格納媒体７

１に格納された暗号化ソフトウェア７３と許諾情報７２の販売を受けることにより、暗号化ソフトウェア７３を平文のソフトウェアに復号し、これを実行する。以下図１４の従来の構成および動作を簡単に説明する。

【０００４】図１４は、従来技術の説明図を示す。図１４において、ソフトウェア格納媒体７１は、暗号化した暗号化ソフトウェア７３およびソフト復号鍵８２を暗号化した許諾情報７２を格納する媒体、たとえば光磁気ディスクであって、ユーザが販売側から購入する対象の媒体である。

【０００５】許諾情報７２は、暗号化ソフトウェア７３を復号して平文のソフトウェアにする情報であって、ソフト復号鍵８２を暗号化したものである。暗号化ソフトウェア７３は、ソフトウェアを暗号化したものである。許諾情報の販売側には、個別鍵生成８１、ソフト復号鍵８２および暗号化回路８３などがある。個別鍵生成８１は、ユーザ計算機のユーザ固有番号（たとえば装置番号）９１をもとにユーザ固有の個別鍵を生成するものである。ソフト復号鍵８２は、暗号化ソフトウェア７３を元の平文のソフトウェアに復号するための鍵である。暗号化回路８３は、ソフト復号鍵８２を、個別鍵生成８１によって生成したユーザ固有の個別鍵によって暗号化した許諾情報７２を生成する回路である。

【０００６】また、ユーザ側のユーザ計算機には、ユーザ固有番号９１、個別鍵生成９２、復号回路９３、ソフト復号鍵９４、および復号回路９５などがある。ユーザ固有番号９１は、ユーザ計算機が持つ固有の番号であって、たとえば装置番号である。個別鍵生成９２は、ユーザ固有番号９１をもとに、ユーザ固有の個別鍵を生成するものである。復号回路９３は、購入したソフトウェア格納媒体７１から読み出した許諾情報７２を復号し、ソフト復号鍵９４を生成するものである。

【０００７】ソフト復号鍵９４は、暗号化ソフトウェア７３を復号して平文のソフトウェアに復号するための鍵である。復号回路９５は、ソフト復号鍵９４をもとに、ソフトウェア格納媒体７１から読み出した暗号化ソフトウェア７３を復号し、元の平文のソフトウェアにするものである。この平文のソフトウェアを、ユーザ計算機の主記憶にローディングし、実行する。

【０００８】つぎに、動作について説明する。

（１）許諾情報の許諾側は、ユーザ計算機の持つユーザ固有番号９１をもとに、個別鍵生成８１がユーザ固有の個別鍵を生成する。この生成した個別鍵をもとに、暗号化回路８３がソフト復号鍵８２を暗号化し、許諾情報７２としてソフトウェアを暗号化した暗号化ソフトウェア７３が格納されたソフトウェア格納媒体７１に書き込む。

【０００９】（２）ユーザは、（１）で許諾情報７２および暗号化ソフトウェア７３の書き込まれたソフトウェア格納媒体７１を購入し、ソフトウェア格納媒体７１を

ユーザ計算機に装着する。個別鍵生成９２がユーザ計算機の持つ固有のユーザ固有番号（たとえば装置番号）９１をもとに、ユーザ固有の個別鍵を生成する。復号回路９３がこの生成したユーザ固有の個別鍵をもとに、購入したソフトウェア格納媒体７１から読み出した許諾情報７２を復号し、ソフト復号鍵９４を生成する。つぎに、復号回路９５がこの生成したソフト復号鍵９４をもとに、ソフトウェア格納媒体７１から読み出した暗号化ソフトウェア７３を復号し、平文のソフトウェアを生成する。この生成した平文のソフトウェアを主記憶にローディングし、実行する。

【００１０】

【発明が解決しようとする課題】上述した図１４の構成の従来の保護方式は、ユーザ固有番号９１を用いており、通常は計算機の固有番号あるいは携帯可能なハードウェアの固有番号を用いている。計算機の固有番号を用いた場合には、許諾情報７２は、計算機に対して実行の許諾を与えていることとなり、この計算機でしか実行できなくなるため、正当なユーザであっても、異なる計算機上では実行が不可能となるという問題が生じている。また、ソフトウェアの譲渡もできない。

【００１１】また、携帯可能なハードウェアの固有番号を用いた場合には、ハードウェア自体および計算機とのインタフェースを設ける必要があり、実施に伴うコストが増加するために実施が困難になるという問題が生じている。

【００１２】本発明は、これらの問題を解決するため、電子化データの媒体に媒体固有番号を持たせ、この媒体固有番号に対して使用する許諾を与え、正規の媒体に格納され、かつ許諾の与えた電子化データのみ実行可能とすることを目的としている。

【００１３】

【課題を解決するための手段】上記目的を達成するため、請求項１の発明にかかる電子化データ保護システムは、使用者側装置で使用される記憶媒体に格納された電子化データを使用許諾者側装置からの使用許諾に基づいて保護する電子化データ保護システムにおいて、前記記憶媒体は、暗号化した暗号化電子化データ並びに当該記憶媒体を一意に特定する媒体固有番号を格納し、前記使用許諾者側装置は、前記記憶媒体に格納した暗号化電子化データを復号するための電子化データ復号鍵と、前記記憶媒体に格納した媒体固有番号に基づいて前記電子化データ復号鍵を暗号化して許諾情報を生成する許諾情報生成手段と、前記許諾情報生成手段により生成された許諾情報を前記記憶媒体に書き込む書込手段と、を備え、前記使用者側装置は、前記記憶媒体から前記許諾情報、暗号化電子化データおよび媒体固有番号を読み取る読取手段と、前記媒体固有番号に基づいて前記許諾情報を復号して前記電子化データ復号鍵を生成する復号鍵生成手段と、前記復号鍵生成手段により生成された電子化デー

タ復号鍵に基づいて前記暗号化電子化データを復号する電子化データ復号手段と、を備えたことを特徴とする。

【００１４】また、請求項２の発明にかかる電子化データ保護システムは、請求項１の発明において、前記許諾情報生成手段および前記復号鍵生成手段は、前記記憶媒体に格納した媒体固有番号に基づいて媒体固有鍵を生成する媒体固有鍵生成手段をそれぞれ備え、前記許諾情報生成手段は、前記媒体固有鍵生成手段により生成された媒体固有鍵に基づいて前記電子化データ復号鍵を暗号化する復号鍵暗号化手段をさらに備え、前記復号鍵生成手段は、前記媒体固有鍵生成手段により生成された媒体固有鍵に基づいて前記暗号化電子化データを復号する復号鍵復号手段をさらに備えたことを特徴とする。

【００１５】また、請求項３の発明にかかる電子化データ保護システムは、請求項１または２の発明において、前記使用許諾者側装置は、前記記憶媒体に格納する複数の暗号化電子化データにそれぞれ対応する異なる電子化データ復号鍵を備え、前記許諾情報生成手段は、前記記憶媒体に格納した媒体固有番号に基づいて使用を許可された暗号化電子化データに対応する電子化データ復号鍵のみを暗号化して許諾情報を生成し、前記復号鍵生成手段は、前記媒体固有番号に基づいて前記許諾情報を復号して前記使用を許可された暗号化電子化データに対応する電子化データ復号鍵を生成することを特徴とする。

【００１６】また、請求項４の発明にかかる電子化データ保護システムは、請求項１、２または３の発明において、前記記憶媒体は、前記使用者側装置による書き替えが不可能な形式で前記媒体固有番号を記憶することを特徴とする。

【００１７】また、請求項５の発明にかかる使用許諾者側装置は、使用者側装置で使用される記憶媒体に格納された電子化データの使用許諾をおこなう使用許諾者側装置において、前記記憶媒体に格納した暗号化電子化データを復号するための電子化データ復号鍵と、前記記憶媒体に格納した当該記憶媒体を一意に特定する媒体固有番号に基づいて前記電子化データ復号鍵を暗号化して許諾情報を生成する許諾情報生成手段と、前記許諾情報生成手段により生成された許諾情報を前記記憶媒体に書き込む書込手段と、を備えたことを特徴とする。

【００１８】また、請求項６の発明にかかる使用許諾者側装置は、請求項５の発明において、前記許諾情報生成手段は、前記記憶媒体に格納した媒体固有番号に基づいて媒体固有鍵を生成する媒体固有鍵生成手段と、前記媒体固有鍵生成手段により生成された媒体固有鍵に基づいて前記電子化データ復号鍵を暗号化する復号鍵暗号化手段と、を備えたことを特徴とする。

【００１９】また、請求項７の発明にかかる使用許諾者側装置は、請求項５または６の発明において、前記記憶媒体に格納する複数の暗号化電子化データにそれぞれ対応する異なる電子化データ復号鍵を備え、前記許諾情報生成手段は、前記記憶媒体に格納した媒体固有番号に基づいて使用を許可された暗号化電子化データに対応する電子化データ復号鍵のみを暗号化して許諾情報を生成することを特徴とする。

【００２０】また、請求項８の発明にかかる使用許諾者側装置は、請求項５、６または７の発明において、前記記憶媒体は、前記使用者側装置による書き替えが不可能な形式で前記媒体固有番号を記憶することを特徴とする。

【００２１】また、請求項９の発明にかかる使用者側装置は、記憶媒体に格納された電子化データを使用許諾者側装置からの使用許諾に基づいて使用する使用者側装置において、前記記憶媒体から当該記憶媒体を一意に特定する媒体固有番号、暗号化された暗号化電子化データ並びに暗号化された許諾情報を読み取る読取手段と、前記媒体固有番号に基づいて前記許諾情報を復号して電子化データ復号鍵を生成する復号鍵生成手段と、前記復号鍵生成手段により生成された電子化データ復号鍵に基づいて前記暗号化電子化データを復号する電子化データ復号手段と、を備えたことを特徴とする。

【００２２】また、請求項１０の発明にかかる使用者側装置は、請求項９の発明において、前記復号鍵生成手段は、前記記憶媒体に格納した媒体固有番号に基づいて媒体固有鍵を生成する媒体固有鍵生成手段と、前記媒体固有鍵生成手段により生成された媒体固有鍵に基づいて前記暗号化電子化データを復号する復号鍵復号手段と、を備えたことを特徴とする。

【００２３】また、請求項１１の発明にかかる使用者側装置は、請求項９または１０の発明において、前記復号鍵生成手段は、前記記憶媒体に格納した媒体固有番号に基づいて前記許諾情報を復号して、当該記憶媒体に格納された複数の暗号化電子化データのうちの使用を許可された暗号化電子化データに対応する電子化データ復号鍵を生成することを特徴とする。

【００２４】また、請求項１２の発明にかかる使用者側装置は、請求項９、１０または１１の発明において、前記記憶媒体は、当該使用者側装置での書き替えが不可能な形式で前記媒体固有番号を記憶することを特徴とする。

【００２５】

【作用】この請求項１にかかる発明によれば、暗号化した暗号化電子化データ並びに当該記憶媒体を一意に特定する媒体固有番号を記憶媒体に格納しておき、使用許諾者側装置は、記憶媒体に格納した媒体固有番号に基づいて電子化データ復号鍵を暗号化して許諾情報を生成し、生成した許諾情報を記憶媒体に書き込み、使用者側装置では、記憶媒体から許諾情報、暗号化電子化データおよび媒体固有番号を読み取り、読み取った媒体固有番号に基づいて許諾情報を復号して電子化データ復号鍵を生成し、生成した電子化データ復号鍵に基づいて暗号化電子

化データを復号するようこととしたので、正規の記憶媒体に格納され、かつ、使用許諾者側装置から許諾を与えられた暗号化電子化データのみを使用者側装置で使用することができる。

【００２６】また、請求項２にかかる発明によれば、記憶媒体に格納した媒体固有番号に基づいて媒体固有鍵を生成し、生成した媒体固有鍵に基づいて電子化データ復号鍵を暗号化するとともに、記憶媒体に格納した媒体固有番号に基づいて媒体固有鍵を生成し、生成した媒体固有鍵に基づいて暗号化電子化データを復号することとしたので、電子化データ復号鍵の暗号強度をより一層高くすることができる。

【００２７】また、請求項３にかかる発明によれば、使用許諾者側装置に、記憶媒体に格納する複数の暗号化電子化データにそれぞれ対応する異なる電子化データ復号鍵を設けておき、記憶媒体に格納した媒体固有番号に基づいて使用を許可された暗号化電子化データに対応する電子化データ復号鍵のみを暗号化して許諾情報を生成するとともに、媒体固有番号に基づいて許諾情報を復号して使用を許可された暗号化電子化データに対応する電子化データ復号鍵を生成することとしたので、一つの記憶媒体に複数の電子化データを格納する場合にも対応することができる。

【００２８】また、請求項４にかかる発明によれば、記憶媒体は、使用者側装置による書き替えが不可能な形式で媒体固有番号を記憶することとしたので、記憶媒体に記憶した暗号化電子化データを他の記憶媒体に複写する不正使用を防止することができる。

【００２９】また、請求項５にかかる発明によれば、記憶媒体に格納した暗号化電子化データを復号するための電子化データ復号鍵を設けておき、記憶媒体に格納した当該記憶媒体を一意に特定する媒体固有番号に基づいて電子化データ復号鍵を暗号化して許諾情報を生成し、生成した許諾情報を記憶媒体に書き込むこととしたので、正規の記憶媒体に格納された暗号化電子化データのみに許諾を与えることができる。

【００３０】また、請求項６にかかる発明によれば、記憶媒体に格納した媒体固有番号に基づいて媒体固有鍵を生成し、生成した媒体固有鍵に基づいて電子化データ復号鍵を暗号化することとしたので、電子化データ復号鍵の暗号強度をより一層高くすることができる。

【００３１】また、請求項７にかかる発明によれば、記憶媒体に格納する複数の暗号化電子化データにそれぞれ対応する異なる電子化データ復号鍵を設けておき、記憶媒体に格納した媒体固有番号に基づいて使用を許可された暗号化電子化データに対応する電子化データ復号鍵のみを暗号化して許諾情報を生成することとしたので、一つの記憶媒体に複数の電子化データを格納する場合にも対応することができる。

【００３２】また、請求項８にかかる発明によれば、記

憶媒体は、使用者側装置による書き替えが不可能な形式で前記媒体固有番号を記憶することとしたので、記憶媒体に記憶した暗号化電子化データを他の記憶媒体に複写する不正使用を防止することができる。

【００３３】また、請求項９にかかる発明によれば、記憶媒体から当該記憶媒体を一意に特定する媒体固有番号、暗号化された暗号化電子化データ並びに暗号化された許諾情報を読み取り、読み取った媒体固有番号に基づいて許諾情報を復号して電子化データ復号鍵を生成し、生成した電子化データ復号鍵に基づいて暗号化電子化データを復号することとしたので、正規の記憶媒体に格納され、かつ、使用許諾者側装置から許諾を与えられた暗号化電子化データのみを使用することができる。

【００３４】また、請求項１０にかかる発明によれば、記憶媒体に格納した媒体固有番号に基づいて媒体固有鍵を生成し、生成した媒体固有鍵に基づいて暗号化電子化データを復号することとしたので、電子化データ復号鍵の暗号強度をより一層高くすることができる。

【００３５】また、請求項１１にかかる発明によれば、記憶媒体に格納した媒体固有番号に基づいて許諾情報を復号して、当該記憶媒体に格納された複数の暗号化電子化データのうちの使用を許可された暗号化電子化データに対応する電子化データ復号鍵を生成することとしたので、一つの記憶媒体に複数の電子化データを格納する場合にも対応することができる。

【００３６】また、請求項１２にかかる発明によれば、記憶媒体は、当該使用者側装置での書き替えが不可能な形式で前記媒体固有番号を記憶することとしたので、記憶媒体に記憶した暗号化電子化データを他の記憶媒体に複写する不正使用を防止することができる。

【００３７】具体的には、図１は、本発明の原理構成図を示す図であり、図１において、媒体１は、暗号化した暗号化電子化データ１４、当該媒体固有の一意の媒体固有番号１２および許諾情報１３を格納するものである。

【００３８】個別鍵生成２１、３１は、媒体固有番号１２から媒体個別鍵を生成するものである。暗号化２３は、媒体個別鍵によって電子化データ復号鍵２２を暗号化するものである。復号３２は、媒体個別鍵によって許諾情報１３を復号して電子化データ復号鍵３３を生成するものである。復号３４は、電子化データ復号鍵３３によって暗号化電子化データ１４を復号し、平文の電子化データを生成するものである。

【００３９】本発明は、図１に示すように、媒体１に予め一意の媒体固有番号１２と共に暗号化した暗号化電子化データ１４を書き込んでおき、許諾側で個別鍵生成２１が媒体の一意の媒体固有番号１２をもとに媒体固有鍵を生成し、暗号化２３がこの媒体固有鍵によって電子化データ復号鍵２２を暗号化し、この暗号化したデータを媒体１に許諾情報１３として書き込み、使用側で個別鍵生成３１が媒体１から読み込んだ媒体固有番号１２もと

に媒体固有鍵を生成し、復号３２がこの媒体固有鍵によって読み込んだ許諾情報１３を復号して元の電子化データ復号鍵３３を生成し、復号３４がこの電子化データ復号鍵３３によって読み込んだ暗号化電子化データ１４を復号し、平文の電子化データにするようにしている。

【００４０】また、一つの媒体１に格納する暗号化電子化データ１４毎に異なる電子化データ復号鍵２２を対応づけ、許諾側で使用を許可する暗号化電子化データ１４の電子化データ復号鍵２２のみを媒体固有鍵によってそれぞれ暗号化し、許諾情報１３として媒体１に格納し、使用側でこの媒体１に格納された許諾情報１３に対応する暗号化電子化データ１４のみを復号し、平文の電子化データにするようにしている。

【００４１】また、媒体固有の一意の媒体固有番号１２を使用側で書き替え不可能な形態で書き込むようにしている。また、暗号化電子化データ１４として、計算機を動作させるソウトウェアあるいは各種データ（文字、画像、音声データなど）を暗号化するようにしている。

【００４２】従って、暗号化電子化データ１４を格納する媒体１に一意の媒体固有番号１２を書き替え不可能な形態で持たせ、この媒体固有番号１２に対して電子化データを使用する許諾を与えることにより、正規の媒体１に格納され、かつ許諾の与えた暗号化電子化データ１４のみの使用を可能とすることができると共に、媒体１に格納されている電子化データの譲渡を可能とし、別の電子計算機に当該媒体１を装填して使用することができる。

【００４３】

【実施例】つぎに、図２から図１３を用いて本発明の実施例の構成および動作を詳細に説明する。ここで、図１で説明した電子化データの例として、計算機に使用するソフトウェアを例に以下説明する。

【００４４】図２は、本発明の１実施例構成図を示す。図２において、ソフトウェア格納媒体１１は、許諾側が使用側に許諾するソフトウェアを格納する媒体であり、たとえば光磁気ディスク（数百Ｍバイトないし数Ｇバイトの容量を持つディスク）などの媒体である。このソフトウェア格納媒体１１には、図示のように、書き替え不可な媒体固有番号１２、使用側にソフトウェアの許諾を与える許諾情報１３、およびソフトウェアを暗号化した暗号化ソフトウェア１５を格納する。

【００４５】媒体固有番号１２は、ソフトウェア格納媒体１１に書き替え不可な一意な媒体固有の番号である。この媒体固有番号１２は、ユーザが書き替え不可能な領域に書き込み、ＯＳが管理するようにしてもよいし、また、ＯＳといえども書き替え不可能な形で予め書き込んだり、一度書き込んだら修正不可のものでもよい。

【００４６】許諾情報１３は、許諾側が使用側にソフトウェアの許諾を与える情報であって、ここでは、暗号化ソフトウェア１５を復号する暗号データである（図６、

図７を用いて詳述する）。

【００４７】暗号化ソフトウェア１５は、ソフトウェアを暗号化したものである（図３から図５を用いて詳述する）。許諾側の計算機には、個別鍵生成２１、ソフト復号鍵２４、暗号化２３などを設ける。

【００４８】個別鍵生成２１は、ソフトウェア格納媒体１１から読み出した媒体固有番号１２をもとに媒体個別鍵を生成するものである（図６を用いて詳述する）。暗号化２３は、個別鍵生成２１によって生成された媒体個別鍵によって、ソフト復号鍵２４を暗号化するものである。この暗号化した暗号データは、ソフトウェア格納媒体１１に許諾情報１３として格納する。

【００４９】使用側の計算機には、個別鍵生成３１、復号３２、ソフト復号鍵３５、復号３４などを設ける。個別鍵生成３１は、ソフトウェア格納媒体１１から読み出した媒体固有番号１２をもとに媒体個別鍵を生成するものである（図６を用いて詳述する）。これは、許諾側の個別鍵生成２１と同じ、媒体個別鍵を生成する。

【００５０】復号３２は、個別鍵生成３１によって生成された媒体個別鍵により、ソフトウェア格納媒体１１から読み出した許諾情報１３を復号し、ソフト復号鍵３５を生成するものである（図８を用いて詳述する）。

【００５１】復号３４は、ソフト復号鍵３５によって、ソフトウェア格納媒体１１から読み出した暗号化ソフトウェア１５を復号し、平文のソフトウェアを生成するものである（図８を用いて詳述する）。この生成した平文のソフトウェアを実行する。

【００５２】以下、図２の構成および動作を順次詳細に説明する。図３は、本発明のソフトウェア格納時のフローチャートを示す。これは、ソフトウェアを作成して暗号化した暗号化ソフトウェア１５および暗号化した許諾情報１３を、ソフトウェア格納媒体１１に格納する時のフローチャートである。

【００５３】図３において、Ｓ１は、ソフトウェアを作成する。これは、メーカがソフトウェア格納媒体に格納するソフトウェア（各種業務プログラム）を作成する。Ｓ２は、ソフトウェア暗号鍵の作成を行う。

【００５４】Ｓ３は、ソフトウェアに対応づけ、暗号鍵管理テーブルに格納する。これは、Ｓ１で作成したソフトウェアのソフトウェア名と、Ｓ２で作成した暗号鍵とを、たとえば図５のソフトウェア暗号鍵管理テーブル４に図示のように対応づけて格納し、統括して管理する。

【００５５】Ｓ４は、指定したソフトウェアに対応したソフトウェア暗号鍵の取り出しを行う。これは、ソフトウェア格納媒体に格納するソフトウェア名に対応するソフトウェア暗号鍵を、図５のソフトウェア暗号鍵管理テーブル４から取り出す。

【００５６】Ｓ５は、Ｓ４で取り出したソフトウェア暗号鍵で、平文のソフトウェアを暗号化し、暗号化ソフトウェアを生成する。これは、たとえば図４に示すよう

に、作成したソフトウェア名とソフトウェア本体のうちソフトウェア本体の部分を、暗号化鍵によって暗号化を行い、図示のようにソフトウェア名と暗号化ソフトウェア本体を作成する。このときの暗号は、ＤＥＳなどを用い、下段に説明したように、換字とビット転置を繰り返して暗号化する。

【００５７】Ｓ６は、メーカ側の格納媒体に暗号化ソフトウェアを格納する。これにより、一度暗号化した暗号化ソフトウェアを保存し、次回以降は、この保存した暗号化ソフトウェアを取り出し、暗号化を省略する。

【００５８】Ｓ７は、暗号化ソフトウェアを読み込み、ソフトウェア格納媒体１１に格納する。Ｓ８は、ソフトウェア格納媒体１１に格納する暗号化ソフトウェアが終わったか判別する。ＹＥＳの場合には、終了する。ＮＯの場合には、Ｓ７を繰り返し行い、指示されたソフトウェア名の暗号化ソフトウェアをソフトウェア格納媒体１１に順次格納する。

【００５９】以上によって、ソフトウェアを作成してこれを暗号化した暗号化ソフトウェアにし、これをソフトウェア格納媒体１１に格納する。図４は、本発明のソフトウェアの暗号化の例を示す。

【００６０】図４の（ａ）は、ソフトウェアの暗号の様子を示す。ここで、ヘッダには、識別子としての役割を行うソフトウェア名などを格納する。このヘッダは、暗号化の対象としない。ソフトウェア本体は、暗号化の対象とし、暗号化鍵によって暗号化して暗号化ソフトウェア本体を作成する。このときの暗号化は、たとえば図示のように、ＤＥＳ(Data Encryption Standerd)を用いる。このＤＥＳは、換字とビット転置を繰り返し、暗号を行う。

【００６１】図４の（ｂ）は、暗号化の様子を示す。暗号化は、ＤＥＳによれば、図示のように６４ｂｉｔのビット列について、暗号化鍵によって暗号化を行い、同じ６４ｂｉｔのビット列を生成する。復号は、復号鍵によって元の６４ｂｉｔのビット列に復号する。

【００６２】図５は、本発明の暗号化ソフトウェアの格納例を示す。図５において、ソフトウェア暗号鍵管理テーブル４は、図３で既述したように、作成したソフトウェア名と、作成した暗号鍵とを対応づけて統括管理するテーブルである。このソフトウェア暗号鍵管理テーブル４には、ソフトウェアが暗号化されていることを表す“ＥＮＣ”を付与したソフトウェア名と、それぞれ６４ビットの暗号鍵をペアにして格納する。

【００６３】以下、動作について説明する。

（１）ソフトウェア格納媒体に格納しようとする平文ソフトウェアについて、ソフトウェア暗号鍵管理テーブル４からソフトウェア暗号鍵を取り出す。

【００６４】（２）暗号化回路４１が渡されたソフトウェア暗号鍵によって、平文ソフトウェアを暗号化する。暗号化は、たとえば図４のＤＥＳを用いて暗号化する。

【００６５】（３）暗号化した暗号化ソフトウェアをソフトウェア格納媒体１１に図示暗号化ソフトウェア１５として格納する。これを指定された全ての平文ソフトウェアについて終了するまで繰り返し行う。この際、一度、暗号化した暗号化ソフトウェアを保存すれば、次回以降からこの保存した暗号化ソフトウェアを取り出してソフトウェア格納媒体１１に格納すればよい。また、媒体固有番号１２は、既述したようにソフトウェア格納媒体１１に固有な一意な番号であって、書き替え不可の形で書き込まれている。また、ソフトウェア暗号鍵管理テーブル４に格納した暗号鍵は、暗号化のアルゴリズムに対象鍵番号を用いた場合には、復号鍵と当該暗号鍵とは一致する。

【００６６】以上によって、平文ソフトウェアについて、ソフトウェア暗号鍵管理テーブル４から該当するソフトウェア暗号鍵を取り出し、これを用いて暗号化を行って暗号化ソフトウェアを作成し、ソフトウェア格納媒体１１に格納する。

【００６７】図６は、本発明の許諾情報の生成フローチャートを示す。これは、許諾しようとするソフトウェアの暗号化した許諾情報１３を生成し、ソフトウェア格納媒体１１に格納するフローチャートである。

【００６８】図６において、Ｓ１１は、許諾しようとするソフトウェア名を入力する。Ｓ１２は、復号鍵管理テーブル５より、ソフト復号鍵を取り出す。これは、図７のソフトウェア復号鍵管理テーブル５から許諾を与えようとするソフトウェア名の復号鍵を取り出す。

【００６９】Ｓ１３は、媒体固有番号の取り出しを行う。これは、許諾情報を書き込もうとする、ソフトウェア格納媒体１１の媒体固有番号を読み出す。Ｓ１４は、媒体個別鍵の生成を行う。これは、右側に記載したように、ソフトウェア格納媒体１１から読み出した平文の媒体固有番号１２について、秘密鍵によって暗号化した媒体個別鍵を生成したり、あるいは平文の媒体固有番号１２について、秘密アルゴリズムによって暗号化した媒体個別鍵を生成したりする。

【００７０】Ｓ１５は、媒体個別鍵によって、ソフト復号鍵を暗号化し、許諾情報を生成する。これは、右側に記載したように、平文のソフト復号鍵について、Ｓ１４で生成した媒体個別鍵により暗号化し、許諾情報を生成する。

【００７１】Ｓ１６は、Ｓ１５で生成した暗号化した許諾情報をソフトウェア格納媒体１１に格納する。以上によって、暗号化ソフトウェア１５を格納したソフトウェア格納媒体１１から媒体固有番号１２を読み出して媒体個別鍵を生成し、ソフト復号鍵についてこの媒体個別鍵で暗号化し、暗号化した許諾情報１３を生成してフトウェア格納媒体１１に格納する。これにより、暗号化ソフトウェア１５および暗号化した許諾情報１３をソフトウェア格納媒体１１に格納したこととなる。

【００７２】図７は、本発明の許諾情報の生成説明図を示す。図７において、ソフトウェア復号鍵管理テーブル５は、暗号化ソフトウェア１５を復号して平文のソフトウェアに復号する際に必要なソフト復号鍵を、ソフトウェア名に対応づけて管理するものである。このソフトウェア復号鍵管理テーブル５には、図５で説明したソフトウェア暗号鍵管理テーブル４と同様の復号鍵を格納する。ここには、暗号化されていることを表す“ＥＮＣ”を付与したソフトウェア名と、それぞれのソフトウェアに対応して６４ビットのソフト復号鍵をペアに格納する。動作について説明する。

【００７３】（１）許諾情報を使用側に販売する場合、まず、ソフトウェア格納媒体１１から媒体固有番号１２を読み出す。この読み出した媒体固有番号１２を個別鍵生成回路２１１に入力し、媒体個別鍵を生成する（図６のＳ１４参照）。

【００７４】（２）つぎに、販売しようとするソフトウェアのソフト復号鍵をソフトウェア復号鍵管理テーブル５から取り出して暗号化回路２３１に入力し、媒体個別鍵で暗号化し、図示許諾情報１３を生成する。この許諾情報１３は、ＥＮＣという暗号化した旨を表す識別子を付与したソフトウェア名と、暗号化した許諾情報とをペアにし、ソフトウェア格納媒体１１に許諾情報１３として格納する。ここで、ソフトウェア復号鍵と、個別鍵生成回路２１１のアルゴリズム（あるいは秘密鍵）は、安全な手段によって保護する。

【００７５】以上によって、許諾側は、ソフトウェア格納媒体１１から読み出した媒体固有番号１２をもとに媒体個別鍵を生成し、この媒体個別鍵をもとに、ソフト復号鍵を暗号化してソフトウェア格納媒体１１に許諾情報１３として格納する。

【００７６】図８は、本発明のソフトウェア復号のフローチャートを示す。これは、使用側が購入したソフトウェア格納媒体１１を計算機に装着し、ソフトウェアを主記憶にローディングして実行するときのフローチャートである。

【００７７】図８において、Ｓ２１は、ソフトウェアの実行命令を受け取る。Ｓ２２は、ソフトウェア格納媒体１１から媒体固有番号１２の取り出しを行う。

【００７８】Ｓ２３は、媒体個別鍵の生成を行う。これは、右側に記載したように、Ｓ２２でソフトウェア格納媒体１１から取り出した媒体固有番号１２について、秘密鍵により暗号化した媒体個別鍵を生成する。あるいは秘密アルゴリズムにより、媒体固有番号１２から暗号化した媒体個別鍵を生成する。

【００７９】Ｓ２４は、Ｓ２３で生成した媒体個別鍵で、ソフトウェア格納媒体１１から読み出した許諾情報１３を復号し、ソフト復号鍵を生成する。これは、右側に記載したように、Ｓ２３で暗号化した媒体個別鍵で、暗号文である許諾情報１３を復号化して平文のソフト復号鍵３５を生成する。

【００８０】Ｓ２５は、ソフトウェア格納媒体１１から暗号化ソフトウェア１５の読み込みを行う。Ｓ２６は、ソフト復号鍵で、Ｓ２５で読み込んだ暗号化ソフトウェア１５を復号し、平文のソフトウェアを生成する。これは、右側に記載したように、暗号文の暗号化ソフトウェア１５について、Ｓ２４で生成したソフト復号鍵３５で復号し、平文のソフトウェアを生成する。Ｓ２７は、ソフトウェア実行する。

【００８１】以上によって、ソフトウェア実行命令に対応して、ソフトウェア格納媒体１１から取り出した媒体固有番号１２から媒体個別鍵を生成し、この媒体個別鍵をもとにソフトウェア格納媒体１１から取り出した許諾情報１３を復元してソフト復号鍵３５を生成し、このソフト復号鍵３５によって、ソフトウェア格納媒体１１から取り出した暗号化ソフトウェア１５を復号して平文のソフトウェアを生成する。この平文のソフトウェアを主記憶にローディングし、実行することが可能となる。

【００８２】図９は、本発明のプログラムの場合の説明図を示す。これは、電子化データとしてプログラムの場合の説明図である。図９の（ａ）は、全体構成図を示す。

【００８３】図９の（ａ）において、光磁気ディスク６は、暗号化プログラムなどを格納するものであって、図２のソフトウェア格納媒体１１に対応するものであり、媒体固有番号１２、許諾情報１３、および暗号化プログラム１６を格納する媒体である。この光磁気ディスク６は、許諾側から購入し、光磁気ディスク装置に装着する。この光磁気ディスク６の他に、光ディスク、ＣＤ－ＲＯＭ、ＦＤ、ＨＤ、磁気テープ、カセットテープなどの記憶媒体であってもよい。

【００８４】プログラムローダ６１は、プログラム命令実行時に、光磁気ディスク６から該当する復号したプログラムを主記憶６３にローディングし、実行可能な状態にするものであって、ここでは、既述した鍵生成（個別鍵生成３１）、復号（復号３２、３４）などを備えた処理部である。

【００８５】主記憶６３は、プログラムローダ６１が光磁気ディスク６から取り出して復号した平文のプログラムを展開するためのＲＡＭ（読み書き可能なメモリ）である。

【００８６】つぎに、図９の（ｂ）のフローチャートに示す順序に従い、図９の（ａ）の構成の動作を説明する。図９の（ｂ）において、Ｓ３１は、プログラム命令実行を受け取る。

【００８７】Ｓ３２は、プログラムローダ６１が実行プログラムを見つけて取り出し、復号する。Ｓ３３は、主記憶上にメモリ展開する。これは、Ｓ３２で復号した平文のプログラムを、主記憶６３上に展開し、動作可能な状態にする。

【００８８】Ｓ３４は、プログラム実行する。Ｓ３３で主記憶６３上に展開された平文のプログラムを実行する。図９の（ｃ）は、ユーザ計算機でのソフトウェア（プログラム）の実行説明図を示す。

【００８９】（１）ユーザ計算機がソフトウェア格納媒体１１から媒体固有番号１２を取り出して個別鍵生成回路３１１に入力し、暗号化した媒体個別鍵を生成する（図８のＳ２３参照）。

【００９０】（２）復号回路３２１が、ソフトウェア格納媒体１１から取り出した図示のような許諾情報１３について、（１）で生成した媒体個別鍵により復号し、図示のようなソフトウェア復号鍵３５１（ソフト復号鍵３５に対応する）を生成する。

【００９１】（３）復号回路３４１が、ソフトウェア格納媒体１１から取り出した暗号化ソフトウェア１５について、（２）で生成したソフトウェア復号鍵３５１により復号し、平文のソフトウェア（プログラム）を生成する。この平文のソフトウェア（プログラム）を主記憶６３に展開し、実行する。

【００９２】ここで、許諾情報１３が格納されていない暗号化ソフトウェア１５は復号することができず、実行不可能である。また、ソフトウェア格納媒体１１を他の媒体の不正にコピーした場合には、媒体固有番号１２が無い、あるいは異なるため、許諾情報１３から正しいソフトウェア復号鍵３５１を復号できず、結果として暗号化ソフトウェアを平文のソフトウェアに復号できず、実行不可能である。尚、ユーザ計算機上では、個別鍵生成回路３１１のアルゴリズムあるいは秘密鍵、生成したソフトウェア復号鍵、復号した平文ソフトウェアは安全な手段によって保護する。

【００９３】図１０は、本発明のデータの場合の説明図を示す。これは、電子化データとしてデータ、たとえば出版物などの文字データ（テキスト）、記号、画像データ、さらに音声データなどの場合の説明図である。

【００９４】図１０の（ａ）は、全体構成図を示す。図１０の（ａ）において、光磁気ディスク６は、暗号化データなどを格納するものであって、図２のソフトウェア格納媒体１１に対応するものであり、媒体固有番号１２、許諾情報１３、および暗号化データ１７を格納する媒体である。この光磁気ディスク６は、許諾側から購入し、光磁気ディスク装置に装着する。この光磁気ディスク６の他に、光ディスク、ＣＤ－ＲＯＭ、ＦＤ、ＨＤ、磁気テープ、カセットテープなどの記憶媒体であってもよい。

【００９５】Ｒ／Ｗモジュール６４は、リード命令実行時に、光磁気ディスク６から該当する復号したデータを主記憶６３に格納するものであって、ここでは、既述した鍵生成（個別鍵生成３１）、復号（復号３２、３４）などを備えた処理部である。主記憶６３は、Ｒ／Ｗモジュール６４が光磁気ディスク６から取り出して復号した平文のデータを格納するためのＲＡＭ（読み書き可能なメモリ）である。

【００９６】つぎに、図１０の（ｂ）のフローチャートに示す順序に従い、図１０の（ａ）の構成の動作を説明する。

【００９７】図１０の（ｂ）において、Ｓ４１は、アプリケーション実行する。Ｓ４２はデータ読み込み命令を実行する。Ｓ４３は、Ｒ／Ｗモジュール６４がデータを見つけ、読み込み復号する。Ｓ４４は、主記憶上に格納する。Ｓ４５は、データの表示、再生を行う。

【００９８】以上によって、Ｓ４２でデータの読み込み命令があったときに、Ｒ／Ｗモジュール６４が、光磁気ディスク６から暗号化データ１７を取り出して復号して平文のデータを生成し、これを主記憶６３に格納する。そして、主記憶６３から取り出してディスプレイ上に出版物の文字列として表示したり、画像を表示したり、音声として発生したりする。つぎに、Ｒ／Ｗモジュール６４の動作を詳細に説明する。

【００９９】図１０の（ｃ）は、ユーザ計算機でのデータの表示／再生説明図を示す。

（１）ユーザ計算機がデータ格納媒体１１１から媒体固有番号１２を取り出して個別鍵生成回路３１１に入力し、暗号化して媒体個別鍵を生成する（図８のＳ２３参照）。

【０１００】（２）復号回路３２１が、データ格納媒体１１１から取り出した図示のような許諾情報１３について、（１）で生成した媒体個別鍵により復号し、図示のようなデータ復号鍵３５２（ソフト復号鍵３５に対応する）を生成する。

【０１０１】（３）復号回路３４１が、データ格納媒体１１１から取り出した暗号化データ１７について、

（２）で生成したデータ復号鍵３５２により復号し、平文のデータ（文字データ、画像データ、音声データなど）を生成する。この平文のデータを主記憶６３に格納し、ディスプレイ上に出版物の文字列、画像、記号として表示したり、音声として発生したりする。

【０１０２】図１１は、ＲＯＭ／ＲＡＭ混在型光磁気ディスクに適用した場合を示す。ＲＯＭ／ＲＡＭ混在型の光磁気ディスクは、図示のように、ユーザ書換え不可能な領域、読み書き可能領域、読み出し専用領域／読み書き専用領域がある。従って、これら領域に図示のように媒体固有番号１２、許諾情報１３、暗号化ソフトウェア１５を格納する。これにより、ユーザ書換え不可能な領域に、媒体固有番号１２を書き込むため、当該光磁気ディスクの固有な媒体固有番号を与え、本発明の保護を図ることができる。

【０１０３】図１２は、本発明の許諾情報を他の格納媒体に格納する場合の例を示す。この場合には、図示のように、ソフトウェア格納媒体に固有な一意の媒体固有番号と、暗号化ソフトウェアのみを予め格納する。そし

て、許諾情報を別の許諾情報格納媒体に格納する。これは、ＣＤ－ＲＯＭなどの書き込む領域を持たない媒体に媒体固有番号および暗号化ソフトウェア（暗号化データ）を予め書き込んでおき、当該ＣＤ－ＲＯＭなどのうちの許諾を与える許諾情報を別の書き込み可能な許諾情報格納媒体（たとえばＦＬＯＰＰＹなど）に書き込む場合の実施例である。

【０１０４】図１３は、本発明の複数のソフトを１枚の媒体に格納する場合の説明図を示す。これは、複数のソフト（あるいはデータ）を１枚の大容量の媒体（光磁気ディスク、ＣＤ－ＲＯＭなど）に格納し、個別販売する場合の実施例である。この場合には、ソフト復号鍵１、２・・・Ｎについて、それぞれ媒体固有鍵によって暗号化した許諾情報１、２・・・Ｎを生成してソフトウェア格納媒体１１に格納する。そして、ユーザは、ソフトウェア格納媒体１１に格納されている暗号化ソフト１、２・・・Ｎのうち、購入希望のソフトウェア名を許諾情報販売側に通知すると、許諾情報販売側はソフトウェアに対応するソフト復号鍵を媒体固有番号から生成した媒体個別鍵で暗号化し、これを許諾情報としてソフトウェア格納媒体１１に格納する。ユーザは、このソフトウェア格納媒体１１を装着し、購入した暗号化ソフトウェアを復号して平文のソフトウェアにし、使用する。一方、ユーザは、許諾情報のないソフトウェアを利用しようとしても暗号化ソフトウェアを復号できず、使用できない。また、他のソフトウェア格納媒体１１の許諾情報をコピーしても、ソフトウェア格納媒体１１の媒体固有番号がコピーできないため、正しい復号ができない。これにより、ソフトウェアの個別販売を行うことが可能となる。

【０１０５】

【発明の効果】以上説明したように、請求項１にかかる発明によれば、暗号化した暗号化電子化データ並びに当該記憶媒体を一意に特定する媒体固有番号を記憶媒体に格納しておき、使用許諾者側装置は、記憶媒体に格納した媒体固有番号に基づいて電子化データ復号鍵を暗号化して許諾情報を生成し、生成した許諾情報を記憶媒体に書き込み、使用者側装置では、記憶媒体から許諾情報、暗号化電子化データおよび媒体固有番号を読み取り、読み取った媒体固有番号に基づいて許諾情報を復号して電子化データ復号鍵を生成し、生成した電子化データ復号鍵に基づいて暗号化電子化データを復号するよう構成したので、正規の記憶媒体に格納され、かつ、使用許諾者側装置から許諾を与えられた暗号化電子化データのみを使用者側装置で使用することが可能な電子化データ保護システムが得られるという効果を奏する。

【０１０６】また、請求項２にかかる発明によれば、記憶媒体に格納した媒体固有番号に基づいて媒体固有鍵を生成し、生成した媒体固有鍵に基づいて電子化データ復号鍵を暗号化するとともに、記憶媒体に格納した媒体固有番号に基づいて媒体固有鍵を生成し、生成した媒体固有鍵に基づいて暗号化電子化データを復号するよう構成したので、電子化データ復号鍵の暗号強度をより一層高くすることが可能な電子化データ保護システムが得られるという効果を奏する。

【０１０７】また、請求項３にかかる発明によれば、使用許諾者側装置に、記憶媒体に格納する複数の暗号化電子化データにそれぞれ対応する異なる電子化データ復号鍵を設けておき、記憶媒体に格納した媒体固有番号に基づいて使用を許可された暗号化電子化データに対応する電子化データ復号鍵のみを暗号化して許諾情報を生成するとともに、媒体固有番号に基づいて許諾情報を復号して使用を許可された暗号化電子化データに対応する電子化データ復号鍵を生成するよう構成したので、一つの記憶媒体に複数の電子化データを格納する場合にも対応することが可能な電子化データ保護システムが得られるという効果を奏する。

【０１０８】また、請求項４にかかる発明によれば、記憶媒体は、使用者側装置による書き替えが不可能な形式で媒体固有番号を記憶するよう構成したので、記憶媒体に記憶した暗号化電子化データを他の記憶媒体に複写する不正使用を防止することが可能な電子化データ保護システムが得られるという効果を奏する。

【０１０９】また、請求項５にかかる発明によれば、記憶媒体に格納した暗号化電子化データを復号するための電子化データ復号鍵を設けておき、記憶媒体に格納した当該記憶媒体を一意に特定する媒体固有番号に基づいて電子化データ復号鍵を暗号化して許諾情報を生成し、生成した許諾情報を記憶媒体に書き込むよう構成したので、正規の記憶媒体に格納された暗号化電子化データのみに許諾を与えることが可能な使用許諾者側装置が得られるという効果を奏する。

【０１１０】また、請求項６にかかる発明によれば、記憶媒体に格納した媒体固有番号に基づいて媒体固有鍵を生成し、生成した媒体固有鍵に基づいて電子化データ復号鍵を暗号化するよう構成したので、電子化データ復号鍵の暗号強度をより一層高くすることが可能な使用許諾者側装置が得られるという効果を奏する。

【０１１１】また、請求項７にかかる発明によれば、記憶媒体に格納する複数の暗号化電子化データにそれぞれ対応する異なる電子化データ復号鍵を設けておき、記憶媒体に格納した媒体固有番号に基づいて使用を許可された暗号化電子化データに対応する電子化データ復号鍵のみを暗号化して許諾情報を生成するよう構成したので、一つの記憶媒体に複数の電子化データを格納する場合にも対応することが可能な使用許諾者側装置が得られるという効果を奏する。

【０１１２】また、請求項８にかかる発明によれば、記憶媒体は、使用者側装置による書き替えが不可能な形式で前記媒体固有番号を記憶するよう構成したので、記憶媒体に記憶した暗号化電子化データを他の記憶媒体に複

写する不正使用を防止することが可能な使用許諾者側装置が得られるという効果を奏する。

【０１１３】また、請求項９にかかる発明によれば、記憶媒体から当該記憶媒体を一意に特定する媒体固有番号、暗号化された暗号化電子化データ並びに暗号化された許諾情報を読み取り、読み取った媒体固有番号に基づいて許諾情報を復号して電子化データ復号鍵を生成し、生成した電子化データ復号鍵に基づいて暗号化電子化データを復号するよう構成したので、正規の記憶媒体に格納され、かつ、使用許諾者側装置から許諾を与えられた暗号化電子化データのみを使用することが可能な使用者側装置が得られるという効果を奏する。

【０１１４】また、請求項１０にかかる発明によれば、記憶媒体に格納した媒体固有番号に基づいて媒体固有鍵を生成し、生成した媒体固有鍵に基づいて暗号化電子化データを復号するよう構成したので、電子化データ復号鍵の暗号強度をより一層高くすることが可能な使用者側装置が得られるという効果を奏する。

【０１１５】また、請求項１１にかかる発明によれば、記憶媒体に格納した媒体固有番号に基づいて許諾情報を復号して、当該記憶媒体に格納された複数の暗号化電子化データのうちの使用を許可された暗号化電子化データに対応する電子化データ復号鍵を生成することよう構成したので、一つの記憶媒体に複数の電子化データを格納する場合にも対応することが可能な使用者側装置が得られるという効果を奏する。

【０１１６】また、請求項１２にかかる発明によれば、記憶媒体は、当該使用者側装置での書き替えが不可能な形式で前記媒体固有番号を記憶するよう構成したので、記憶媒体に記憶した暗号化電子化データを他の記憶媒体に複写する不正使用を防止することが可能な使用者側装置が得られるという効果を奏する。

【図面の簡単な説明】

【図１】本発明にかかる原理構成図である。

【図２】本発明にかかる１実施例構成図である。

【図３】本発明にかかるソフトウェア格納時のフローチャートである。

【図４】本発明にかかるソフトウェアの暗号化の例である。

【図５】本発明にかかる暗号化ソフトウェアの格納例である。

【図６】本発明にかかる許諾情報の生成フローチャートである。

【図７】本発明にかかる許諾情報の生成説明図である。

【図８】本発明にかかるソフトウェア復号のフローチャートである。

【図９】本発明にかかるプログラムの場合の説明図である。

【図１０】本発明にかかるデータの場合の説明図である。

【図１１】ＲＯＭ／ＲＡＭ混在型光磁気ディスクに適用した場合である。

【図１２】本発明にかかる許諾情報を他の格納媒体に格納する場合の例である。

【図１３】本発明にかかる複数ソフトを１枚の媒体に格納する場合の説明図である。

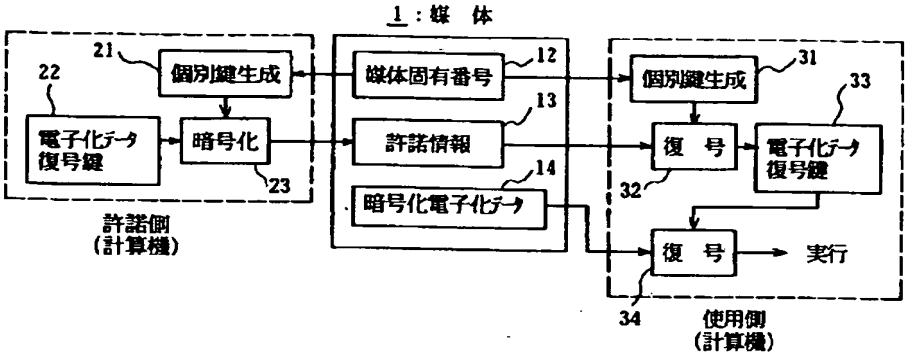
【図１４】従来技術の説明図である。

【符号の説明】

１　媒体
１１　ソフトウェア格納媒体
１１１　データ格納媒体
１２　媒体固有番号
１３　許諾情報
１４　暗号化電子化データ
１５　暗号化ソフトウェア
１６　暗号化プログラム
１７　暗号化データ
２１　個別鍵生成
２１１　個別鍵生成回路
２２　電子化データ復号鍵
２３　暗号化
２３１　暗号化回路
２４　ソフト復号鍵
３１　個別鍵生成
３１１　個別鍵生成回路
３２　復号
３２１　復号回路
３３　電子化データ復号鍵
３４　復号
３４１　復号回路
３５　ソフト復号鍵
３５１　ソフトウェア復号鍵
３５２　データ復号鍵
４１　暗号化回路
６　光磁気ディスク
６１　プログラムローダ
６３　主記憶
６４　Ｒ／Ｗモジュール

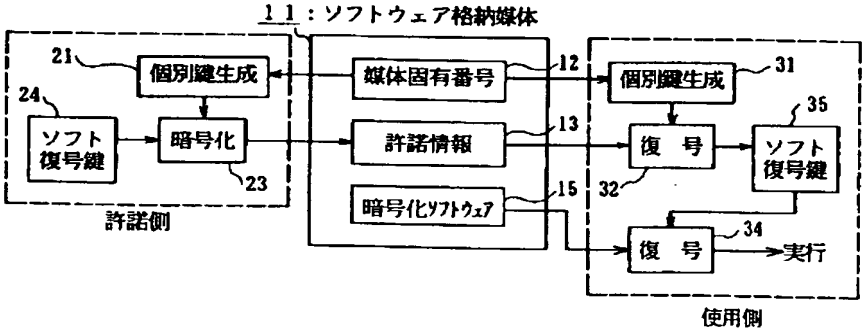
【図１】

本発明の原理構成図



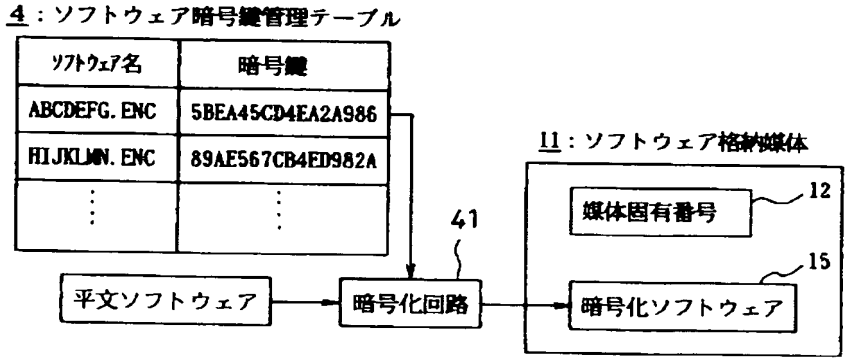
【図２】

本発明の１実施例構成図



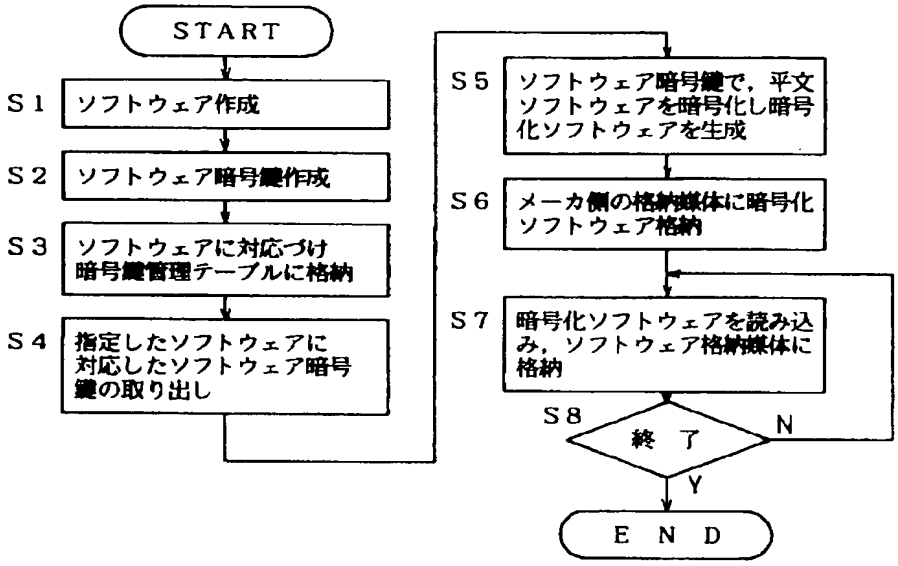
【図５】

本発明の暗号化ソフトウェアの格納例



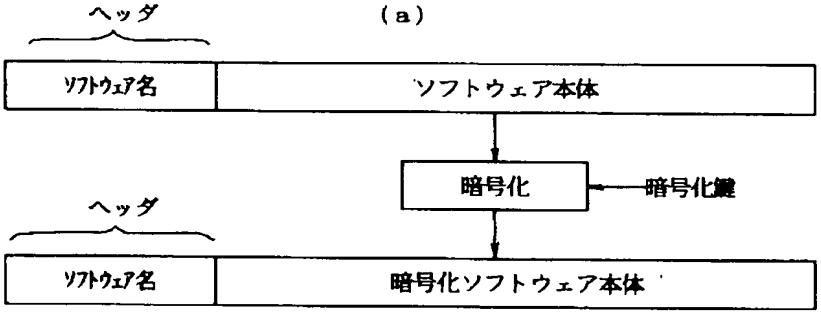
【図３】

本発明のソフトウェア格納時のフローチャート

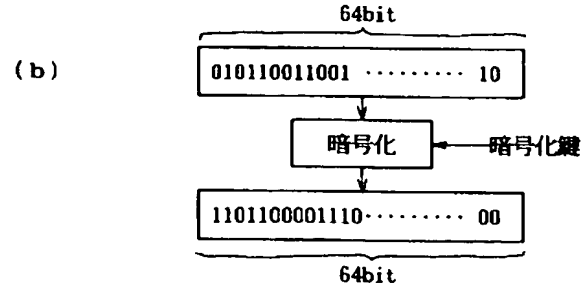


【図４】

本発明のソフトウェアの暗号化の例

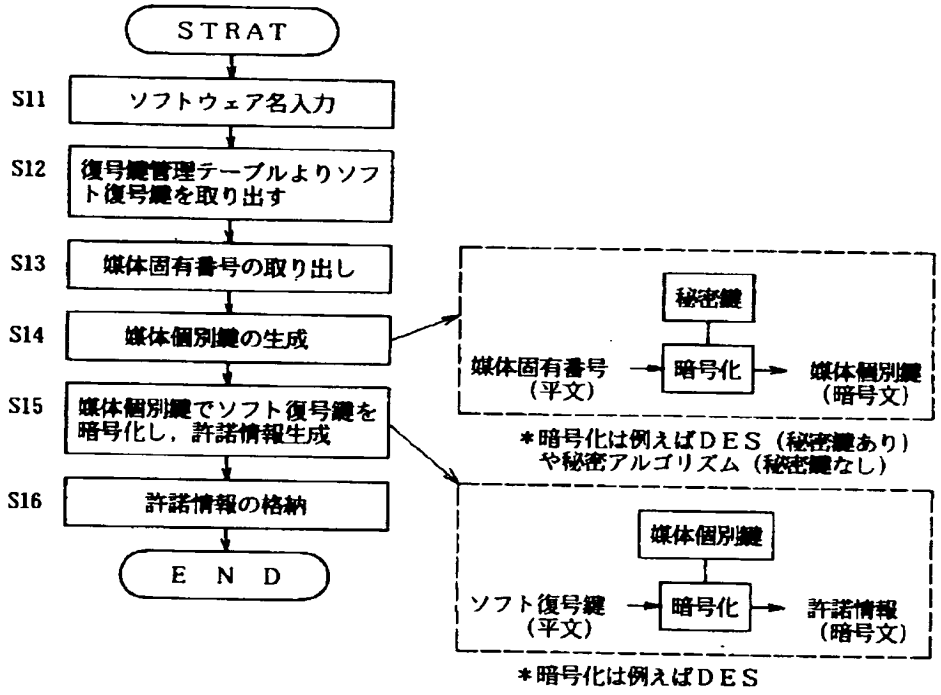


暗号化には，例えばＤＥＳ(Data Encryption Standerd)を用いる。
ＤＥＳは，換字とビット転置を繰り返し，暗号化を行う。



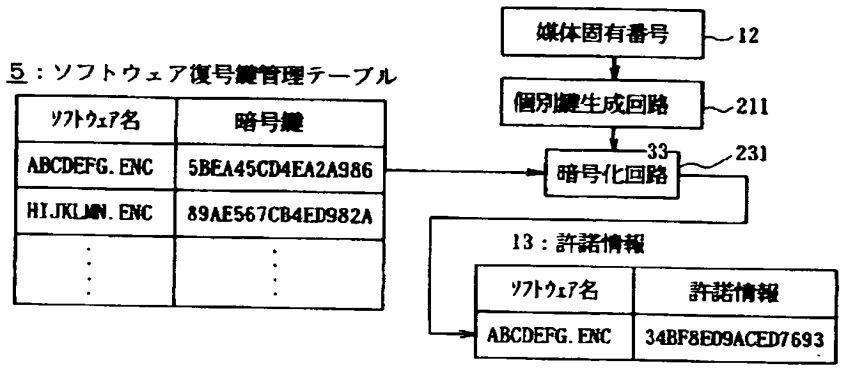
【図６】

本発明の許諾情報の生成フローチャート



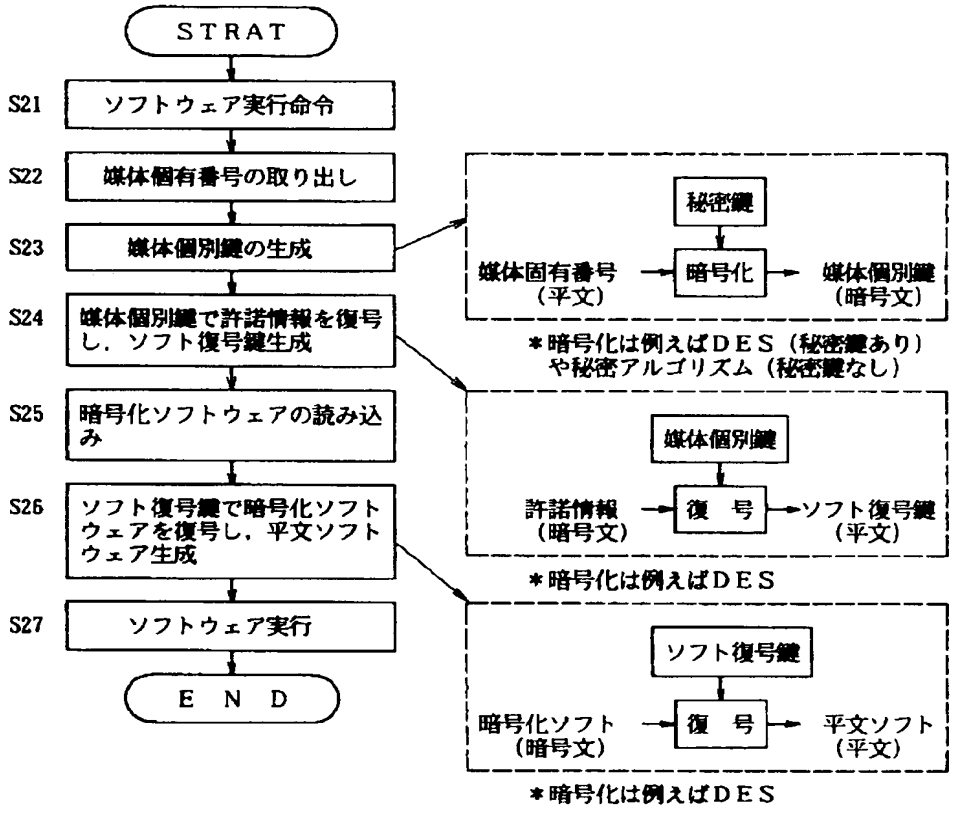
【図７】

本発明の許諾情報の生成説明図



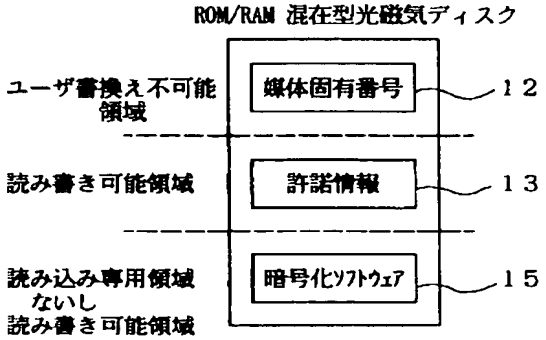
【図８】

本発明のソフトウェア復号のフローチャート



【図１１】

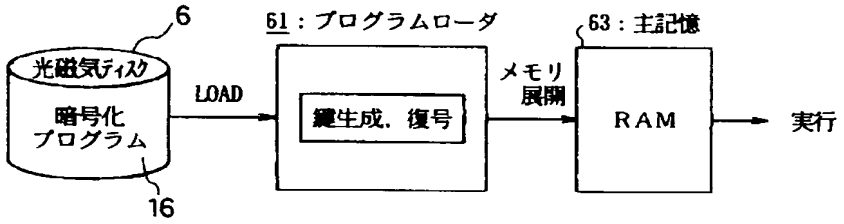
ROM/RAM 混在型光磁気ディスクに適用した場合



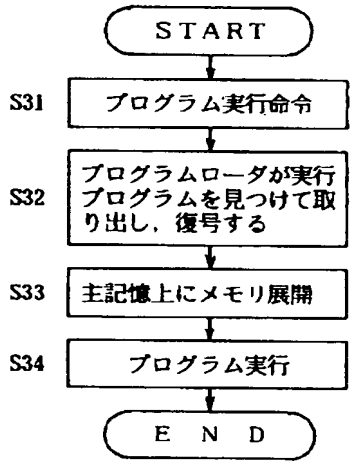
【図９】

本発明のプログラムの場合の説明図

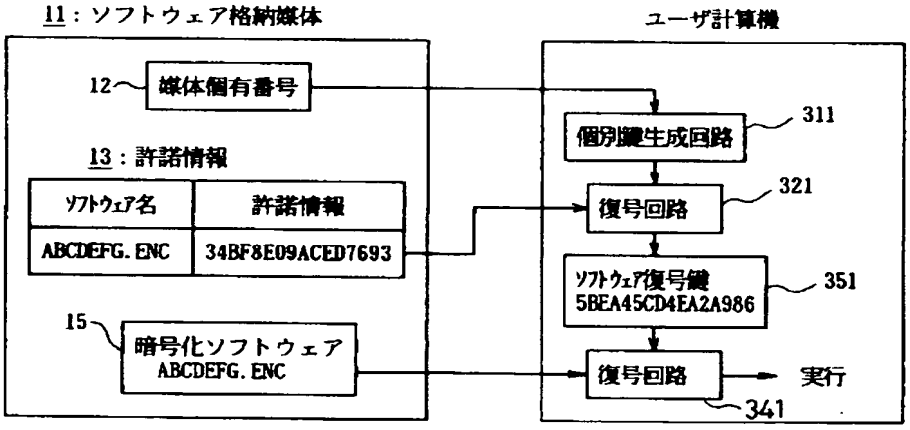
（ａ）全体構成図



（ｂ）動作フローチャート



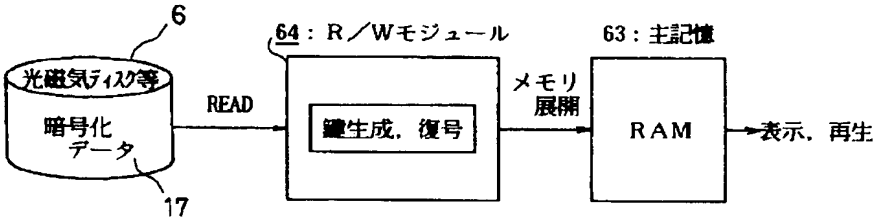
（ｃ）ユーザ計算機でのソフトウェアの実行説明図



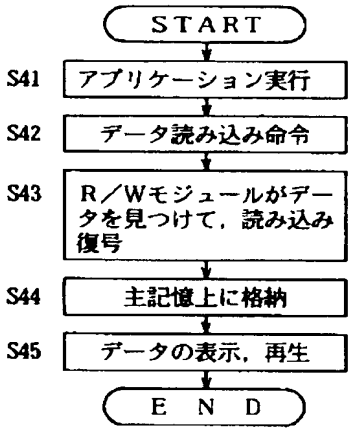
【図１０】

本発明のデータの場合の説明図

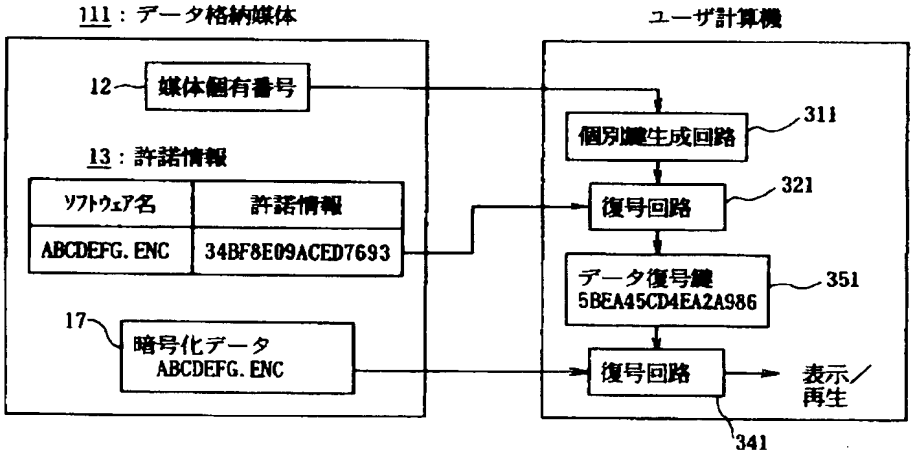
（ａ）全体構成図



（ｂ）動作フローチャート

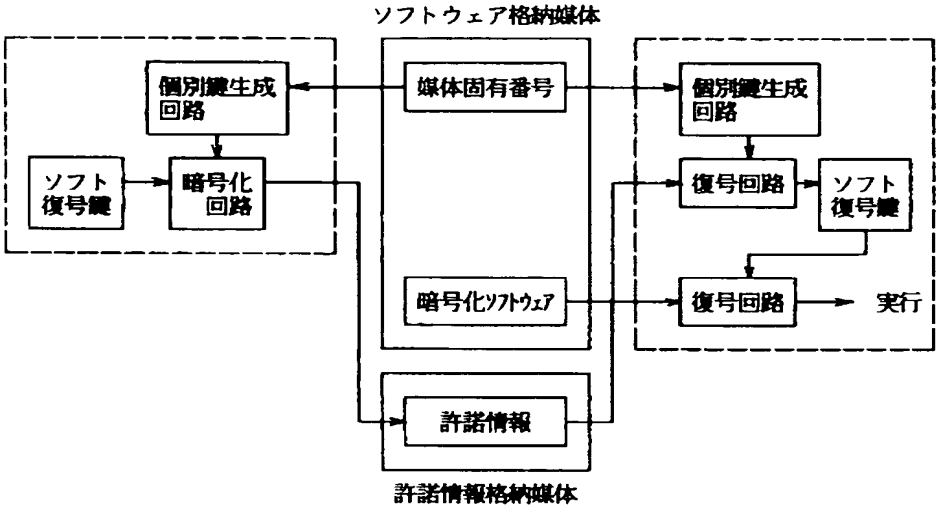


（ｃ）ユーザ計算機でのデータの表示／再生説明図



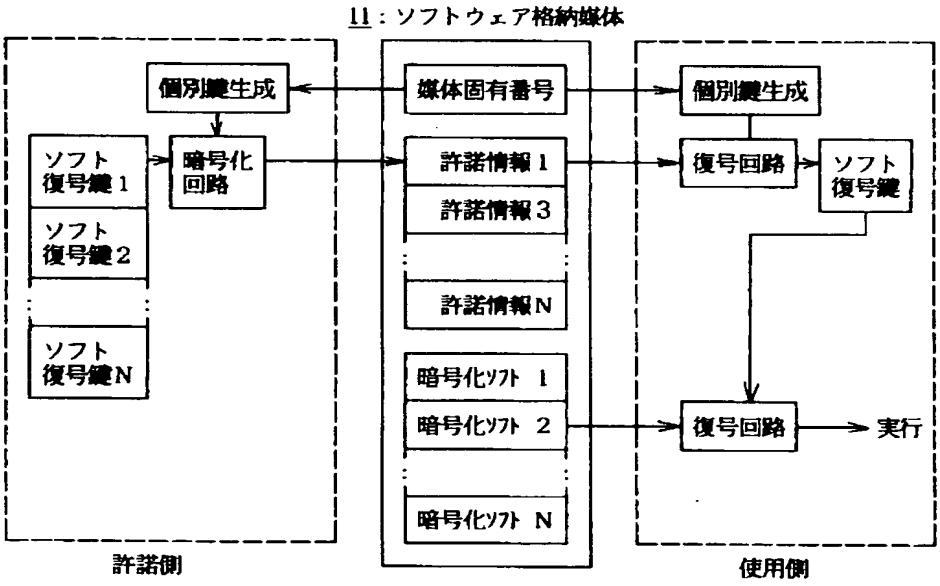
【図１２】

本発明の許諾情報を他の格納媒体に格納する場合の例



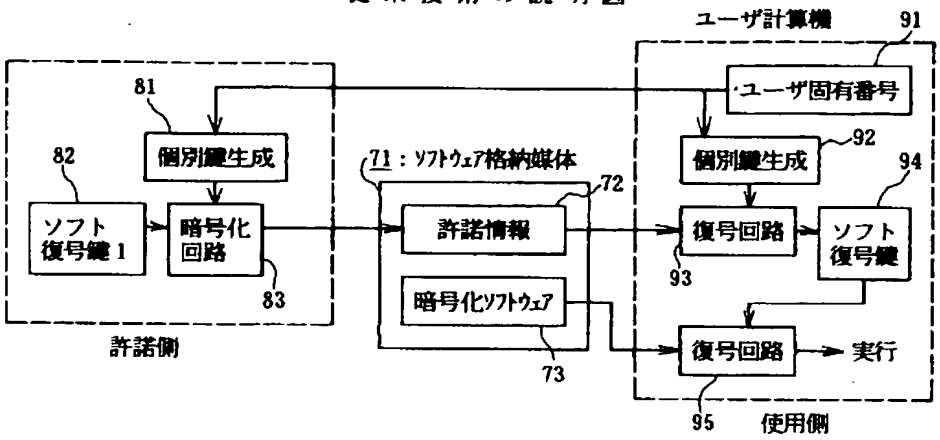
【図１３】

本発明の複数のソフトを１枚の媒体に格納する場合の説明図



【図１４】

従 来 技 術 の 説 明 図



フロントページの続き

(56)参考文献　特開　平３－30020（ＪＰ，Ａ）
特開　昭62－108629（ＪＰ，Ａ）
特開　平１－194029（ＪＰ，Ａ）
特開　昭62－226335（ＪＰ，Ａ）
特開　昭61－204807（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.⁷，ＤＢ名)
G06F　12/14
G06F　9/06
G09C　1/00
G06F　15/21